ELECTRONIC BANKING FRAUD IN KENYA: A CRITIQUE OF THE SUFFICIENY OF THE LAW

NJIRU EMILY MUKAMI

G62/68907/2011

LLM Thesis Submitted in Partial Fulfillment of the Requirements for the Award of the Degree of Master of Laws of the University of Nairobi

2014

SCHOOL OF LAW

UNIVERSITY OF NAIROBI

NAIROBI

DECLARATION

I **NJIRU EMILY MUKAMI,** do hereby declare that this is my original work and that it has not been submitted for award of a degree or any other academic credit in any other University.

NJIRU EMILY MUKAMI

G62/68907/2011

Signed.....13/08/2014 Date.....13/08/2014

This thesis has been submitted for examination with my approval as a University supervisor.

DR. WINNIE KAMAU

Signed....Wkamau..... Date...13/8/2014....

TABLE OF CONTENTS

ACKNOWLEDGMENTS

My heartfelt gratitude goes to all those who contributed in making this study a success. I profusely thank the Board of Post-Graduate Studies, University of Nairobi for granting me fully paid scholarship to pursue my Master of Laws (LL.M) Degree. In me you have planted a seed of wisdom which will live through the generations.

Immerse gratitude goes to my supervisor, *Dr. Winnie Kamau*. I will always remain indebted to you for accepting to supervise this work. Thank you for walking with me through this journey. The knowledge and wisdom you have imparted on me will always remain in my memory. Your endless guidance, patience, untiring reading has made this work worth reading. May God bless you abundantly.

To you Geoffrey Sore, thank you for accepting to assist me in my research. Your thoughts provided the critique necessary to refine this work and enhance its quality. I am grateful for your insightful input and your unending desire to see the completion of this work.

To my family, especially my husband and mentor, *Henry Kamau*, thank you for your ever present support. Every single day you have stood by me, your constant reminders of my obligation to complete this work kept me on toes. Thank you for your emotional, moral and physical support. Your belief in me enabled me to push on and rise up to this challenge. Indeed I am immensely grateful. To my *mum,* for your daily prayers on all your children, for your everyday sacrifices that enables us have a more comfortable life than you, for believing in each one of us, I will forever be indebted to you.

Above all, honour and glory goes to my Heavenly Father, for the gift of life and gift of all of you who have assisted me in different ways. Indeed I can do all things through Christ who strengthens me! This Thesis would not have been completed but for your grace. Thank you for taking me through every step of my life.

DEDICATION

This thesis is dedicated to my late father, *Wanaruona Senior*. 20 years are gone, but the seed of hope you planted 29 years ago has sprouted to bring in your desired dream of faith, determination, hardwork and courage. Thank you for believing in me. I have grown to be the person you desired. Even as you lie silently in peace, I know you are watching! Great are those who plant seed in their lifetime for their spirit never dies! Dad your greatness surpasses any power of hopelessness. May you forever Rest in Peace.

ABBREVIATION AND ACRONYNMS

ATM	Automated Teller Machine
CAK	Communications Authority of Kenya
CCK	Communications Commission of Kenya
CBK	Central Bank of Kenya
CFA	Computer Fraud and Abuse Act
CID	Criminal Investigation Department
EBG	Electronic Banking Group
ECT	Electronic Communications and Transactions Act
EFT	Electronic Funds Transfer
EFTPOS	Electronic Funds Transfer at Point of Sale
DNS	Deferred Net Settlement
KCB	Kenya Commercial Bank
KEPSS	Kenya Electronic Payment and Settlement System
KIC	Kenya Information and Communications Act
PIN	Personal Identification Number
RTGS	Real Time Gross Settlement system
SA	South Africa
UK	United Kingdom
USA	United States of America

UNCITRAL United Nations Commission on International Trade Law Model Law on Electronic Commerce

LIST OF STATUTES AND REGULATIONS

KENYA

Banking Act, Chapter 488 Laws of Kenya

Central Bank of Kenya Act, Chapter 491 Laws of Kenya

Cheque Act, Chapter 35 Laws of Kenya

Evidence Act, Chapter 80 Laws of Kenya

Kenya Information and Communications Act, Chapter 411A Laws of Kenya

Law of Contract Act, Chapter 23 Laws of Kenya

National Payment System Act, Act no. 39 of 2011

Penal Code, Chapter 63 Laws of Kenya

Banking (Credit Reference Bureau) Regulations, 2008

Civil procedure Rules of 2010

The Central Bank of Kenya Prudential Guideline

AUSTRALIA

Australian Spam Act, 2003

Criminal Code of Western Australia,1913

Criminal Code 2002, Australian Capital Territory

New South Wales Crimes Act,1900

UNITED KINGDOM

Computer Misuse Act, 1990

Data Protection Act, 1998

Fraud Act 2006

Theft Act 1968

SOUTH AFRICA

Electronic Communications and Transactions Act, 2002

National Credit Act 34 of 2005

UNITED STATES

Computer Fraud and Abuse Act, 1986

Gramm-Leach-Bliley Act of 1999

Privacy Act, 1974

INTERNATIONAL

Basel Accord

United Nations Commission on International Trade Law Model Law on Electronic Commerce

TABLE OF CASES

KENYA

Central Bank of Kenya Limited v Trust Bank Limited & 4 others Civil Appeal No.215/96

Joseph Kyenze v. Cliff Ondari & 2 others (2007) eKLR

John Ngugi Gathumbi V Republic (2010) eKLR

UNITED KINGDOM

Derry v Peek (1889) 14 App. Cas. 337

Hedley Byrne &? Co Ltd v Heller and Partners Ltd, (1964) AC 465

HIH Casualty & General Insurance Ltd & Ors v Chase Manhattan Bank & Ors (2003) UKHL 6

Miller v Minister of Pensions [1947] 2 ALLER 372

Oxford v Moss (1979) 68 Cr App R 183

R v Ghosh (1982) QB 1053

R v Landy (1981) 1 WLR 355

R v preddy (1996) AC 815

Scott v Metropolitan Police Commissioner [1975] AC 819

Williams (1953)1 QB 660 (CCA)

SOUTH AFRICA

Diners Club SA (Pty) Ltd v Singh and another 2004 (3) SA 630

S v Myeza 1985 (4) SA 30 (T)

S v Van den Berg 1991 (1) SACR 104 (T)

S v Salcedo 2003 (1) SACR 324

PAPUA NEW GUINEA

Papua New Guinea Reg v Jamieson [1975] P.N.G.L.R. 216.

Kasaipwalova v The State (1977) PNGLR 257

AUSTRALIA

O'Sullivan (1925) V.l.R. 514 , 518

Penfolds Wines Pty Ltd v Elliott (1946) 74 CLR 204, 214

Pollard v Commonwealth DPP (1992)28 NSWLR 659

R v Glenister (1980) 2 NSWLR 597

R v Licardy unrep, 28/09/94, NSWCCA

INDIA

T. K. Dutta vs. Pawan Kumar Didwani and Anr (1995) CRI. L. J. 3274

NEW ZEALAND

R v Wilkinson (1999)1 NZLR 403

UNITED STATES

America Online v IMS 24 Fsupp 2d 548 (ED Va, 1998)

America Online, Inc. v. LCGM, Inc. 46 F. Supp. 2d 444

CompuSewe Inc. v Cyber promotions 962 F Supp 1015 (SD Ohio, 1998)

Mundy v Decker (1999) WL 14479

United States v. Williams 458 U.S. (1982) 279,290

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND OF THE STUDY

Electronic banking fraud in Kenya has become a major challenge.[1] This crime is on the increase and is a matter of concern not only to the banks but to the public in general.[2] This is because fraud costs are passed on to the society through increased customers inconveniences, opportunity costs, unnecessary high prices as well as occurrence of criminal activities funded by the fraudulent gains. Deloitte Forensic director Robert Nyamu in his interview with Business Daily correspondent stated that, "the magnitude of fraud is going up and this may be predominantly, caused by the sophistication of fraud and how it is being managed." Billions of shillings have been lost by the banks in fraud alone.[3] A report by Business Daily indicates that Kenyan banks were a victim of more than half of the 4.1 billion shillings that hit the East African banks in the year 2011.[4]

Most of the fraud perpetrated in the banks is technology driven. Previously, most of the transactions in the banks were paper driven. In order to keep abreast with the emerging technology, banks have wholesomely embraced technology. There has been great technological development in the banking sector in Kenya since 2000.[5] For example, Real Time Gross Settlement system (RTGS) an electronic payment system, went live in Kenya on 29th July, 2005.[6] Further, the cheque truncation system was introduced in

---

[1] "Pushing Banks from Old ATM Cards to High Security Chip and Pin Card Technology in Kenya" CIO/East Africa Magazine, 6th November 2012 online at http://www.cio.co.ke/news/top-stories/pushing-banks-from-old-atm-cards-to-high-security-chip-and-pin-card-technology-in-kenya (Visited 20th May 2013).

[2] Wesley K. Wilhelm & Fair I. Company, "The Fraud Management Lifecycle Theory: A Holistic Approach to Fraud Management." *Journal of Economic Crime Management* 2, no. 2 (2004): 1.

[3] See, David Mugwe, *Kenyans Banks Biggest Victims Of Sh 4.1 bn Fraud,* Business Daily, 31st July 2012 online at http://www.businessdailyafrica.com/Kenyan-banks-biggest-victims-of-Sh4bn-fraud-/-/539552/1467902/-/9kmes9z/-/index.html (visited 23rd June 2013).

[4] *Ibid.*

[5] Electronic Funds Transfer was introduced in August 2000, see Nyangosi Richard, Nyang'au Samuel and Magusa Hellen "Managing Banks Amid Information and Computer Technology: Paradigms in Kenya." online at http://www.aibuma.org/archive/proceedings2011/aibuma2011_submission_43.pdf (visited 25th June 2013).

[6] See https://www.centralbank.go.ke/index.php/2012-09-21-11-44-41/kepss (visited 22nd May, 2014).

2011.[7] These technological advancement were necessitated by the need to keep abreast with the developments in the banking industry internationally.

1.2 STATEMENT OF THE PROBLEM

It is in no doubt that banks have substantially embraced technology in their operations. This has rendered the banking system or the transactions thereof more vulnerable to fraud. Consequently, there has been an increase in the occurrence of electronic banking fraud. This study appreciates that technology precedes the law. Indeed the rapid development of technology globally has led to an increase in new forms of national and transnational crimes.[8] Consequently, there is a need to come up with appropriate proposals on how best to regulate electronic banking fraud with a futuristic focus on mind.

Kenya lacks specific laws on electronic banking fraud. The Penal Code, which is the main criminal statute does not provide for the offence of electronic banking fraud. One can only interpret some of the offences therein in a broad manner to encompass the various nature and manifestations of electronic banking fraud. Some of those offences include forgery, obtaining by false pretense and theft. The 2009 amendments attempted to enlarge the scope of applications of fraud to include fraud perpetrated through electronic means. This was by way of enlarging the scope of the offence of forgery as provided for under section 347 of the Penal Code to include fraudulently making or transmitting electronic records. The regulating against forgery of electronic records was a good attempt in the fight towards electronic banking fraud since the amendment captures at least an aspect of electronic banking fraud which is altering electronic data and presenting it as genuine with an aim of gaining a financial advantage. However, generally the Penal Code is insufficient to deal with the offence of electronic banking fraud.

---

[7] Central Bank of Kenya *Annual Report* (Nairobi, 2012) P.58.

[8] Tengku M. T, "Ethics of Information Communication Technology." p.3. A paper presented at the the Regional Meeting on Ethics of Science and Technology 5-7 November 2003, Bangkok. Online at http://www.unescobkk.org/elib/publications/ethic_in_asia_pacific/239_325ETHICS.PDF (visited 17th February 2012).

The banking Act which is the main statute that regulates banking business in Kenya does not delve into the realms of possible banking crimes and prohibiting them thereof. The Act does not provide for electronic banking fraud.

1.3 OBJECTIVES

The main objective of this study is to examine the existing legal framework in Kenya that addresses electronic banking fraud and assess its effectiveness thereof. The study shall also make recommendations on the way forward.

Specifically, this study seeks to explore the following objectives:

i. To examine the nature and various forms of electronic banking fraud.
ii. To identify and examine the existing legal framework relevant in electronic banking fraud.
iii. To assess the effectiveness of the examined legal framework.
iv. To draw vital lessons that may be informative from other jurisdictions on how they have addressed the issue of electronic banking fraud.
v. Make recommendations for reforms.

1.4 RESEARCH QUESTIONS

The study seeks to address the following questions;

i. What is the nature of electronic banking fraud?
ii. What form does the electronic banking fraud take?
iii. What is the existing legal framework in Kenya that seeks to address electronic banking fraud?
iv. How effective is the current legal framework in addressing electronic banking fraud?
v. What lessons can be learnt from other jurisdictions necessary to address the menace of electronic banking fraud?

Kenya in an attempt to interrogate the role of law in addressing the crime of electronic banking fraud. There is no study that has been done in Kenya specifically to interrogate the existing legal framework relevant in addressing electronic banking fraud with an aim of finding its sufficiency or otherwise. Consequently there is a notable knowledge gap in this area and hence my research. This study will inform policy in relation to finding a better legal framework necessary to address the crime of electronic banking fraud in Kenya.

1.7 CONCEPTUAL FRAMEWORK

Electronic banking has been defined as the use by the banks of electronic channels for receiving instructions and delivering their products and services to their customers.[14] Others have defined it specifically in relation to funds transfer as any transfer of funds initiated or processed using electronic techniques.[15] For the purposes of this paper however, electronic banking fraud encompasses fraud committed through the use of various banking technologies. Some of the technologies includes *inter alia* telephone banking and internet banking.

1.8 THEORETICAL FRAMEWORK

Fraud in banking has been the subject of research by a number of scholars. Different approaches have been propagated in an attempt to address the crime of electronic banking fraud. The first approach aims at reducing or eliminating fraud in banking. This is a prohibitive or preventive approach which is advanced by writers who seek to some extent use the law to stop the crime of fraud in banking from happening.[16] These are the 'fraud management' proponents.[17]

---

[14]Basel Committee on Baking Supervision, "Management and Supervision of Cross-Border Electronic Banking Activities," *Bank for International Settlement* (July 2003).

[15] Kilonzo KD, "Analysis of the Legal Challenges posed by Electronic Banking." *Kenya Law Review*, 1(2007):333.

[16] ACI Payment System, *Fighting Wire Fraud: An Industry Perspective* online at http://www.aciworldwide.com/-/media/files/collateral/fighting-wire-fraud-v1-tl-us-5143-0613.ashx (visited on 30th June 2014).

[17] V Subha, "Retail Banking Fraud Management: Challenges and Emerging Alternatives." *TATA Consulty Services,* (2012).

Proponents of the fraud management theory look for ways of preventing fraud. They aim at combating the vice as opposed to dealing with the consequences. *Subha V*,[18] for instance, proposes that the key in combating fraud in banking lies in right sourcing and sharing the best practices amongst the banks. Others emphasize on instigating criminal sanctions.[19] They advocate that the criminal justice system should prohibit fraud in banking and impose heavy penalties. The criminal procedure system should permit fraudsters to be apprehended and convicted with ease.

The other proponents of the preventive theorist suggest that all banks must abide by law in order to prevent fraud. They borrow from experts in technology and propose particular measures that banks must put in place to shield themselves from fraud. Among the proponents is *Kömmerling O and Kuhn M* who, for instance, advocate for coming up with 'fraud resistant ATM cards.[20] The preventive approach of compacting fraud has been criticized in that it is idealist and does not deal with problems occasioned by fraud in banking.[21] The approach is seen as unrealistic and unachievable in that it would be impossible to have a society free and devoid of banking fraud.

The second theory is the risk sharing approach which constitutes of the liberalist and the positivist. The liberal approach has been propagated by *Nicholas Bohm, Ian Brown and Brian Gladman*[22]. The authors argue that the law should be such that either party carries the fault depending on the extent of their fault in the occurrence of the fraud.[23] The fault in this case is mainly negligence. To them, the extent of risk born by either the bank or the customer is directly proportional to the extent to which they are at fault and not according to the contract between the bank and the customer. They oppose the positivist

---

[18] *Ibid.*

[19] See, The Growing Global Threat of Economic and Cyber Crime, The National Fraud Center, Inc, in conjunction with the Economic Crime Investigation Institute, Utica College, Dec 2000.

[20] O Kömmerling & M Kuhn, "Design Principles for Tamper-Resistant Smartcard Processors." Proceedings of USENIX Workshop on Smartcard Technology, (Chicago, USA, May 1999).

[21] Kurdas C, Does Regulation Prevent Fraud? The Case for Manhattan Hedge Fund, The Independent Review, v. 13, n. 3, Winter 2009,p. 12. The writer uses the case to demonstrate that fraud cannot be stopped by merely having laws and regulations in place.

[22] Bohm Nicholus , Brown Ian & Gladman Brian, "Electronic Commerce: Who Carries the Risk of Fraud?" *Journal of Information, Law and Technology* 3, (2000).

[23] *Ibid* p.32.

approach of allocation of risks purely on the agreement between the two because of the possibility of unfair contracts.[24]

The positivists on the other hand tend to promote the allocation of risk based on the construction of the contract between the bank and customer. They argue that the contract between the bank and the customer should always be enforced. To the extreme end of this school, it doesn't matter that the contract is fair or not. All that matters is that the contract was duly signed.[25]The positivist approach tends to ignore the fact that the bank and the customer are not at equal bargaining power while making the contract. In fact, not many people go through the terms and references of the contract, leave alone trying to understand them.

The third theory as proposed by *Peter Alces* is a realistic approach to the bank-customer relationship.[26] The author proposes that realist principle to payments legislations best accommodates the interests of the bank and the customer. The author posits that legislations on bank-customer relationship are either pro-financial institution or consumer protectionist. He highlights the contradiction of the US law on payment systems by stating that the law regulating the use of cheques in payment is particularly pro-financial institution[27] whereas the ones regulating electronic transfers and credit cards are consumer protectionist.[28]

It is evident that both the preventive and the risk sharing approaches may not be the best approaches. The preventive approach is targeted towards elimination of the banking fraud entirely. Neither technology nor the law can completely eliminate or deter fraudsters. The 'risk sharing' theorists are also deficient in that there is a lack of balance between consumer protection and the need to respect the freedom of contract. This is because the positivists propose that the contract between the bank and the customer should be the sole

---

[24] *Ibid.*

[25] Rhoades and Sinon, Electronic Banking Fraud, www.rhoadssinon.com/media/site_files/35_PABanker%2001-02.pdf (Visited 3rd June 2013).

[26]Peter Alces, "Toward a Jurisprudence of Bank-Customer Relations" *The Wayne Law Review*, 299 (1968).

[27]Art 31 and 42 of the Uniform Commercial Code (UCC).

[28] The author cites the Electronic Fund Transfer Act of 1978 (E.F.T.A.).

instrument of determining who bears the risk and to what extent. On the other hand the liberalist posit that the bank and the customer are at different bargaining powers and thus the contract cannot be relied upon in total.

This paper takes a realistic approach to legislations that seek to address banking fraud. The paper seeks to achieve the missing link between the preventive approach and the risk sharing approach. The paper acknowledges the need to use legislation to prevent fraud in banking but at the same time accept that it is not possible to eliminate it all together. The paper also takes cognizance of the role and place of contract between the bank and the customer. The aim is to have fraud in banking at its lowest possible level and a structure of risk sharing that is fair to both the bank and customer and the society as a whole.

1.9 LITERATURE REVIEW

A number of scholars have written on electronic banking and some have in their work related that with banking fraud. Some scholars interrogate the question of the sufficiency of the law in addressing electronic banking fraud whereas others are more concerned with fraud generally. A congruent point for all of them is that fraud in banking is a challenge that needs to be addressed and this may be achieved through proper legislation. They however differ on what constitutes proper law or how to make the current laws more effective in curbing banking fraud generally.

Njaramba Gichuki in his book, *Law of Financial Institutions in Kenya*[29] recognizes that electronic banking has brought in new challenges to the financial sector. Part 111 of the book specifies some of the emerging issues in the banking industry especially those brought about by the use of technology in the banks. The author enlists some of these banking technologies such as the use of Automated Teller Machine (ATM) cards, electronic funds transfer at point of sale (EFTPOS) cards, telephone banking including mobile money transfer services. The author has also dedicated a chapter on some of the new technologies adopted by the banks. He defines new technology banking as the

[29] Gichuki Njaramba, *Law of Financial Institutions in Kenya*, 2nd ed. (Nairobi: Law Africa, 2013).

conduct of traditional banking through the mobile phone or through the computer. The book identifies challenges brought about by new technology banking. Some of these includes partial or complete none face to face mode of communication between the bank and the customers.[30] My study goes further to suggest that as a result of adoption of these technologies by the banks hence the changing nature of bank-customer relationship, the banks and the customers thereof have been left more vulnerable to electronic banking fraud.

Gichuki appreciates that that there is deficient of the law with regard to regulating issues brought about by modern technology.[31] My study proposes that electronic banking fraud is one of the new challenges faced in the banking industry as a result of the usage of new technology. Consequently, this paper interrogates the applicable laws if any that seeks to address electronic banking fraud and assess its efficiency/sufficiency or otherwise.

David Ormerod in his book, *Smith and Hogan's Criminal Law*[32], discusses various criminal offences as found in the United Kingdom (UK) statutes. Of particular relevance is the analysis of the Fraud Act, 2006 which provides a clear definition of what constitutes fraud.[33] My study accepts the definition of fraud as encapsulated in the Act and goes further to recommend the approach by the UK to enact a specific law on fraud as one of the mechanism through which Kenya can legislate against electronic banking fraud by enacting a general fraud law. The author further examines the Computer Misuse Act, 1990 as amended by the Serious Crimes Act 2007.[34] The Act mainly legislates against the unauthorized access to a computer with intent to commit or facilitate commission of an offence and unauthorized modification of computer materials. My study goes further to analyze the Data Protection Act, 1998 which *inter alia* criminalizes the act of knowingly or recklessly obtaining or disclosing personal data or procuring its obtaining without the consent of data controller. One of the ways through which

---

[30] Chapter 14, p 253-261.
[31] *Ibid.*
[32] David Ormerod, *Smith and Hogan's Criminal Law* 13th ed. (New York: Oxford University Press, 2011).
[33] Ibid, para 23.1.1. at 870.
[34] *Ibid,* 1046-1047.

electronic banking fraud is propagated is through impersonation by using another person's password or personal information. My study analyses the Data Protection Act with an aim of finding out its relevance or otherwise for the purposes of building useful suggestions in the Kenyan context.

Michael Brindle & Raymond Cox in their book, *Law of Bank Payments*[35] discusses banking fraud generally without particular reference to electronic banking fraud.[36] The book further discusses the effects of fraud in terms of the person who bears the risk of fraud and the burden of proving fraud.[37] The book also identifies some new banking technologies that have been adopted by the banks such as the electronic funds transfer, use of electronic money in terms of smart cards and prepaid cards and internet banking. My study shows how those banking technologies are prone to electronic banking fraud. Further, my study identifies various manifestations of electronic banking fraud and the applicable law in Kenya that attempt to combat this kind of banking fraud.

Kethi D. Kilonzo in her paper, *An analysis of the Legal Challenges posed by Electronic Banking*[38] asserts that the Banking Act does not define the term electronic banking fraud. She restates the important role played by technology in the banks. Some of the benefits brought about by electronic banking as identified by her includes 24 hour access to their accounts, use of digital signatures, use of Automated Teller Machines, electronic pay roll systems, direct transfers, telephone and internet banking.[39] The writer argues a case for documentation of electronic transfer which she contends remains unregulated in Kenya. She further acknowledges that there are apparent risks prevalent in electronic banking. However, she only addresses the risk of a customer who incurs loss where one's ATM is used without the consent of the owner. In this regard she suggests that banks ought not to be wholly absolved of the loss incurred. She argues that the law is not sufficient in this

---

[35] Michael Brindle & Raymond Cox, *Law of Bank Payment* 4th ed. (London: Sweet & Maxwell, 2010).
[36] *Ibid,* p. 385.
[37] *Ibid,* p .839.
[38] Kethi D. Kilonzo, "An analysis of the Legal Challenges posed by Electronic Banking" *Kenya Law Review,* 1(2007):323.
[39] *Ibid* p.326.

regard.[40] Specifically on electronic banking, the writer acknowledges that there are no specific laws governing electronic commerce or electronic payments in Kenya.

My study isolates the risk of electronic banking fraud as a key challenge brought about by use of technology in the banks. My study further acknowledges that there is no specific law in Kenya that addresses electronic banking fraud and the existing laws can only be interpreted in a manner that recognizes electronic banking fraud. My study therefore proceeds by first analyzing the existing legal framework that attempt to address electronic banking fraud with an aim of investigating its sufficiency and making recommendations thereof.

Nicholas Bohm, Ian Brown and Brian Gladmanin in their paper, *'Electronic Commerce: Who Carries the Risk of Fraud?'* advocates that the law in traditional banking transactions should be replicated in the modern electronic banking transactions. They hold that the law is fair and sufficient as concerns fraud in the traditional paper banking transactions.[41]However, in electronic banking, they hold that the risk of loss of money due to fraud in banking is largely borne by the customer. The paper therefore proposes that the law in traditional transactions in banking should inform the law in electronic banking. This historical approach suggests that common law principles and early statutes on banking apply to electronic banking.[42]

Whereas this paper suggests that the traditional banking methods mainly paper based should inform electronic banking my study suggests otherwise. My study proposes that electronic banking poses new challenges and the solutions for addressing banking fraud lies over and above the paper based system of banking.

---

[40] *Ibid,* p.333.

[41] Bohm Nicholus , Brown Ian & Gladman Brian, " Electronic Commerce: Who Carries the Risk of Fraud?" *Journal of Information, Law and Technology* 3, (2000).

[42] The law that deals with the traditional banking transactions in the United Kingdom is the Bill of Exchange Act 1882 which largely replicates the common law position. The general rule is that, with forged documents and specifically cheques, the bank bears the risk. For instance under section 24 of the Act, it is immaterial that the bank took all reasonable security measures to ensure authenticity of a cheque.

Owalabi SA in his paper, *Fraud and Fraudulent Practices in Nigeria Banking Industry*[43] dedicates his research to analyzing the various forms of fraudulent practices in the Nigerian banking industry. The research also mentions various legislations targeted at reducing fraud. The paper raises loopholes of the Nigerian banking legal instruments without necessarily providing legal solutions. My research however is dedicated towards scrutinizing Kenyan legal framework that seeks to address banking fraud with an aim of providing legal solutions.

Ajayi M.A in his paper, *Determinants of Fraud in Nigerian Banking Industry*[44], identifies fraud as very widespread in the Nigerian banking industry. The paper specifically examines the relationship between staff and the widespread offence of fraud and forgery in the Nigerian banking industry. He further identifies various measures adopted by the banks to combat banking fraud. The paper basically recognizes the increased occurrences of banking fraud and recommends possible measures that the banks can use to combat the problem. My study, however, specifically interrogates the offence of electronic banking fraud. It differentiates between the general fraud offence and electronic banking fraud which it isolates as a very widespread in the light of the emergence of various new technologies which banks have adopted.

Further Steven M. Biskupic has written a paper on, *Fine Tuning the Bank Fraud Statute: A Prosecutor's Perspective* [45] which suggests redrafting of the banking fraud laws so that they reflect the new fraud activities brought in by modern banking. He states that legal verbiage is what makes the law on fraud ineffective in handling fraud in banking.[46] The writer highlights two USA cases to illustrate his conviction one being *United States v. Williams*[47] whereby the prosecution case failed because of the legal complexities

---

[43] Owalabi SA, "Fraud and Fraudulent Practices in Nigeria Banking Industry." *African Research Review Journal*, 4. No. 3b (2001)*: 240, 253-254.*

[44] Ajayi M. A *Determinants of Fraud in Nigerian Banking Industry* Univerisity of Ilorin, Nigeria):101 online at http://www.unilorin.edu.ng/publications/ajayima/8.pdf (visited 17th June, 2014).

[45] See generally Biskupic Steven M., "Fine Tuning the Bank Fraud Statute: A Prosecutor's Perspective." *Marq. L. Rev.* 82, (1999) :381.

[46] *Ibid.* P. 24.

[47] 458 U.S. 279,290 (1982).

presented by the term 'execution' in the 18 U.S.C. § 1344 (1998) which is the Federal statute on bank fraud. The author states that good legal drafting of the fraud laws will heal the inefficiencies of fraud in banking. My study just like Biskupic highlights areas where there are weaknesses of the law but in addition provide legal solutions to the same.

1.10 RESEARCH METHODOLOGY

This study relies on both the primary and secondary data. Our main source of primary data is the Constitution, statutes, regulation and the cases. The primary data will be mainly library based supplemented by some limited field work in order to gain certain information necessary for arriving at an informed conclusion. The study is also heavily reliant on secondary data. Secondary data is mainly through written material on the topic where important data is recorded. Most of the data needed in this study is captured in writing and it will be useful in drawing conclusions, analyzing the situation and putting forward what needs to be done.

1.11 CHAPTER BREAKDOWN

This study is composed of five chapters. Chapter one is the introduction consisting of the study background, statement of the problem, justification of the study, research objectives and the hypothesis, literature review, conceptual framework, theoretical framework and the methodology of data collection.

Chapter two defines electronic banking fraud its nature and various manifestation. This chapter gives an insight as to some of the forms of electronic banking fraud and how they are perpetrated. This chapter helps in understanding the nature of electronic banking fraud.

Chapter three gives an overview of the existing legal framework in Kenya that seeks to address electronic banking fraud. This chapter looks at the relevant Kenyan statutes and any regulations thereof. It also discusses relevant aspects of international law useful in combating electronic banking fraud. The chapter also discusses briefly the key institutions in Kenya that are charged with the mandate of investigating electronic

banking fraud. The aim of this chapter is to analyse the applicable law with an aim of finding out the extent to which the law addresses electronic banking fraud.

Chapter four seeks to draw various lessons that can be learnt from other jurisdictions in addressing electronic banking fraud. This will be by way of finding out how other jurisdictions have used the law to address this crime. This will be very informative in drawing our conclusion and making recommendations thereto.

Chapter five will consist of conclusion and recommendations whereby specific recommendations shall be made and a way forward advanced.

CHAPTER TWO

FORMS AND NATURE OF ELECTRONIC BANKING FRAUD

2.1 INTRODUCTION

This chapter discusses various forms of electronic banking fraud and its various manifestations. The chapter commences by describing the nature of fraud generally, highlighting its' distinct elements that characterizes it. This chapter also defines fraud both in the criminal context and as a civil liability highlighting any distinguishing characteristic if any and pinpointing any similarities if at all. The definition part sums up by defining fraud in the context of electronic banking fraud. This is by way of discussing various ways through which banks use technology so as to create an understanding as to how electronic banking fraud is perpetrated. The chapter then concludes by discussing various forms and nature of banking fraud and giving examples where applicable.

2.2 DEFINITION

2.2.1 Fraud

The Black's Law Dictionary defines fraud as:

> "a knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment. A misrepresentation made recklessly without belief in its truth to induce another person to act." [48]

This definition puts a lot of emphasis on the making of a false statement whether by words or conduct as the core ingredient of the offence of fraud.

The House of Lords in the United Kingdom has defined fraud to mean "to deprive a person dishonestly of something which is his or of something he is or would or might but

[48] *Black's Law Dictionary*, (9th ed, 2009).

for the perpetration of the fraud be entitled to."[49] The emphasis here is on the word deprive and dishonest. This means that as a result of the dishonest conduct of someone else a person is denied that which would have been ordinarily theirs had the dishonest conduct never occurred.

Lord Herschell in the classical case of *Derry v Peek*[50] rightly emphasized the core elements of the crime of fraud when he stated that:

> "First, in order to sustain an action in deceit, there must be proof of fraud and nothing short of that will suffice. Secondly, fraud is proved when it is shown that the false representation has been made (i) knowingly, (ii) without belief in its truth, or (iii) recklessly, careless whether it be true or false. Although I have treated the second and third as distinct cases, I think the third is bit an instance of the second, for one who makes a statement under such circumstances can have no real belief in the truth of what he states. To prevent a false statement from being fraudulent, there must, I think, always be an honest belief in its truth."

The judge in this case seems to emphasize the characterization of fraud being the making of a false statement whether knowingly or carelessly. It is immaterial whether the victim suffers loss or not.

The elements of fraud have been summarized as follows:

i. Misrepresentation of a material fact;

ii. Made with knowledge of its falsity ;

iii. Made with intent to induce the victim to rely on the misrepresentation ;

iv. The victim relies upon the misrepresentation ; and

v. The victim suffers damages as a result. [51]

---

[49] *Scott v Metropolitan Police Commissioner* [1975] AC 819 at 839.
[50] (1889) 14 App. Cas. 337 at 376.
[51] Association of Certified Fraud Examiners, "The Fraud Trial: The Law Against Fraud" P. 6 online at http://www.acfe.com/uploadedFiles/Shared_Content/Products/Self-Study_CPE/Fraud-Trial-2011-Chapter-Excerpt.pdf (Visited 25th September 2013).

Having analyzed all the above cited definitions it is clear that the word fraud has no definite meaning. However, there seems to be distinct elements which are ordinarily present (though not in all cases) for there to be fraud. To begin with there has to be a false statement either made knowingly or recklessly without caring as to its truth. Secondly, the false statement must be made with the intention of inducing another to act on it. Thirdly, a person should act on the misrepresented fact and as a result suffers loss or injury.

2.2.2 Fraud in the Civil Context

Fraud in the civil context centers on the fraud laws that regulate interpersonal relationship.[52] Fraud as a civil wrong is committed against another person, whether natural or a corporation, as opposed to a wrong against the state or the public.

In Kenya, civil fraud takes a number of dimensions in different branches of law. For example, fraud is one of the factors that vitiate a contract. Where there is a fraudulent misrepresentation that entices a person to enter into a contract, the innocent party is entitled to vitiate the contract and seek damages. Section 2 of the Law of Contract Act[53] recognizes the applicability of the English common law to contracts in Kenya.

Lord Bingham in the case of *HIH Casualty & General Insurance Ltd & Ors v Chase Manhattan Bank & Ors*[54] held that:

> "...fraud is a thing apart. This is not a mere slogan. It reflects an old legal rule that fraud unravels all. It also reflects the practical basis of commercial intercourse. Once fraud is proved, it vitiates judgments, contracts and all transactions whatsoever."

Chitty has also stated that, "Fraud is a vitiating element in a contract. It is also a tort. It follows that the plaintiff who proves fraudulent misrepresentation is entitled to rescind the contract and may in addition be entitled to recover damages."[55]

---

[52] The legal dictionary defines civil law as, 'A body of rules that delineate private rights and remedies, and govern disputes between individuals in such areas as contracts, property, and Family Law; distinct from criminal or public law.' http://legal dictionary.thefreedictionary.com/civil+law (visited 7th July 2013).
[53] Cap 23 Laws of Kenya.
[54] (2003) UKHL 6, p. 15.

Fraud can also arise as a tort due to fraudulent misrepresentation or what is called tort of deceit. Misrepresentation cases can be prosecuted either under criminal law or civil law.[56] For example, under criminal law one can be convicted for the offence of false pretense which is derived from the making of a fraudulent misrepresentation. Where a defendant makes a false representation, knowing it to be untrue, or being reckless as to whether it is true, and intends that the claimant should act in reliance on it, then in so far as the latter does so and suffers loss the defendant is liable for that loss.[57]

In civil cases one should show that the plaintiff not only relied on the false statement but actually suffered loss as a result of such reliance. This should be contrasted with negligent misrepresentation which occurs if a plaintiff suffers loss because of careless or negligence of another party who makes a representation which the plaintiff was entitled to rely on it.[58] A fraud case may not be based on negligent or innocent misrepresentation. Innocent misrepresentation is where the representor honestly believes in truth of the statement and had reasonable ground for the belief.

Fraud as a tort may also take the form of fraudulent conveyances. In the case of *Joseph Kyenze v. Cliff Ondari & 2 others*[59], Lady Justice Mary Angawa revoked a title of land registered in the names of the defendants on grounds that it had been fraudulently acquired and ordered the land to be registered in the name of the plaintiff. This was a case of a fraudulent conveyance where the defendants had fraudulently transferred the land, which was the subject of the suit.

---

[55] Chitty Joseph, *Chitty on Contracts* 22nd ed Vol 1(London: Sweet & Maxwell, 1961) para 273.
[56] Association of Certified Fraud Examiners, *The Fraud Trial: The Law Against Fraud* P. 10 available at http://www.acfe.com/uploadedFiles/Shared_Content/Products/Self-Study_CPE/Fraud-Trial-2011-Chapter-Excerpt.pdf (Visited 25th September 2013).
[57] A.M. Jones , M.A. Dugdale, *Clerk & Lindsell on Torts* 19th ed. (London: Sweet & Maxwell, 2005) para 18-01.
[58] See the case of *Hedley Byrne & Co Ltd v Heller and Partners Ltd,* (1964) AC 465.
[59] *[2007] eKLR.*

Under Order 2 rule 10 of the Civil Procedure Rules 2010, a party who asserts fraud must plead specifically particulars of any misrepresentation or fraud stating clearly in the facts how the alleged fraud occurred. Similarly the standard of proof in civil cases is higher than on a balance of probabilities but lower than the criminal threshold of proof which is beyond reasonable doubt. In the case of *Central Bank of Kenya Limited v Trust Bank Limited & 4 others*[60], the Court of Appeal held that, "fraud and conspiracy to defraud are very serious allegations. The onus of the prima facie proof was much heavier on the appellant in this case than in an ordinary civil case."

In the case of *Miller v Minister of Pensions*[61] Lord Denning held that:

> "The degree is well settled. It must carry reasonable degree of probability, but not so high as is required in criminal case. If the evidence is such that the tribunal; can say, 'we think it more probable than not,' the burden is discharged, but, if the probability is equal, it is not."

2.2.3 Fraud in the Criminal Context

There is no definition of the word fraud in the Penal Code. The Code only outlines several crimes that involve fraud, such as, conspiracy to defraud[62], intent to defraud[63], frauds in the public service[64], marriage with fraudulent intent[65] and fraudulent disposition of mortgaged goods[66].

Stephen in his book, *A History of the Criminal Law of England*[67], has defined fraud in the following words:

> "...whenever the words "fraud" or "intent to defraud" or "fraudulently" occur in the definition of a crime two elements at least are essential to the commission of the crime:

---

[60] Civil Appeal No.215/96.
[61] [1947] 2 ALL ER 372.
[62] Section 317 of the Penal Code.
[63] Section 348 of the Penal Code.
[64] See section 127 of the Penal Code.
[65] See section 172 of the Penal Code.
[66] See section 291 0f the Penal Code. Other criminal frauds include fraudulently dealing with minerals in mines, fraudulent appropriation of power, conspiracy to defraud, frauds on sale, frauds by trustees, fraudulent accounting etc. These are all under the Penal Code.
[67] Stephen, *A History of the Criminal Law of England*, vol. II (London: Macmillan 1883) p. 121.

namely, first, *deceit or an intention to deceive or in some cases mere secrecy and secondly, either actual injury or possible injury or an intent to expose some person either to actual injury or to a risk of possible injury* by means of that deceit or secrecy." [68] [Emphasis added]

Fraud in the criminal context can stand either as the *mens rea* of a crime or as the *actus reus* crime. Where the words "fraudulently" or "intent to defraud" are used, they describe the *mens rea* of certain crimes. For example section 172 of the Penal Code states that,

> "Any person who dishonestly or with a fraudulent intention goes through the ceremony of marriage, knowing that he is not thereby lawfully married, is guilty of a felony and is liable to imprisonment for five years."

The *mens rea* in this case is the fraudulent intention and the *actus reus* on the other hand is going through the ceremony of marriage.

Section 115 and 127 on the other hand denotes circumstances when fraud is the *actus reus.* Section 115 states that,

> "Any person *who practises any fraud* or deceit, or knowingly makes or exhibits any false statement, representation, token or writing to any person called or to be called as a witness in any judicial proceeding, with intent to affect the testimony of such person as a witness, is guilty of a misdemeanour." [Emphasis added]

Section 127 on the other hand states,

> "Any person employed in the public service who, in the discharge of the duties of his office, *commits any fraud* or breach of trust affecting the public, whether the fraud or breach of trust would have been criminal or not if committed against a private person, is guilty of a felony." [Emphasis added]

These two examples depict circumstances when fraud is the *actus reus* on itself. This shows that when fraud appears as the main crime and not just an element, the law may use such terms as "committing any fraud" or "practicing fraud". Here, the crime itself is fraud and it is not just an element of another crime.

---

[68] *Ibid* p. 121.

In the Indian case of *T. K. Dutta vs. Pawan Kumar Didwani and Anr*[69] the bail was cancelled in view of the fact that the accused obtained bail by practising fraud on Court. In denying him bail, the court had this to state,

> "...The opposite party No. 1 accused clearly, therefore, had obtained the aforesaid order of bail dated 10th May, 1993 on the aforesaid false /frivolous plea taken in his aforesaid fresh application filed on 10th May, 1993, and on the said submissions made before the Court on his behalf, which was nothing short of practising fraud upon the Court for obtaining the said Order."

In this case just like the Penal Code, practicing fraud is the actus reus.

In criminal fraud, the standard of proof is beyond reasonable doubt and it is upon the prosecution to prove. In the case of *John Ngugi Gathumbi V Republic*[70] Lady Justice J.N Khaminwa quashed the conviction and set aside the sentence of the appellant on grounds that the prosecution had not proved all the counts to the required standard that is beyond reasonable doubt. In this case the appellant had been charged with making of a false document with intent to defraud contrary to section 345 of the Penal Code.

It must be noted that most of the fraud acts are both civil and criminal wrongs and one may seek remedies from either or both the civil and criminal regimes.[71] For example obtaining by false pretense is a criminal offence and the same can be prosecuted under the law of contract where a party makes a false representation which becomes a term of contract. The major difference between civil and criminal fraud is the question of criminal intent. In a civil fraud, the plaintiff has to show that, because a misrepresentation was believed and acted upon, actual damages, personal or financial, were suffered. In criminal fraud, the damage or loss suffered is not a condition precedent for sustaining a conviction for fraud since the fraud contemplated may only be an attempt or the dishonest conduct

---

[69] *(1995) CRI. L. J. 3274.*
[70] *2010] eKLR.*
[71] See generally Teal E. Luthy, "Assigning Common Law Claims for Fraud." *Law Review*, 65 no.3, (1998): 1001, 1028.

In criminal fraud a person need not show that they acted on a false misrepresentation, all what is required to be proved is that the misrepresentation was made with fraudulent intention.[72] The fraudulent intent can be deduced from the very act of making a dishonest statement or from the possibility of occasioning loss or injury on reliance of such statement. The similarity is that in both civil and criminal fraud there is the existence of a false or dishonest statement made by one person to another either by words or conduct.

2.2.4 Electronic Banking Fraud

Electronic banking fraud has already been defined under the conceptual framework as encompassing fraud committed through the use of various banking technologies. Banking technology refers to the use of refined information and communication technologies together with computer science to enable banks to offer better services to its customers in a secure, reliable, and affordable manner, and sustain competitive advantage over other banks.[73]

Thus bank fraud that manifests in or is conducted through any of the banking technologies, as opposed to the traditional paper banking methods such as the use of cheques and cash, is electronic banking fraud. The fact the instructions are transmitted over through various means of technology or through the internet rather than through face to face communication means that the banks and the customers are more vulnerable to electronic banking fraud since there is a possibility that the person actually transacting is an imposter. The banking technologies are manifested through the mode of banking and especially in regard to payment systems. Examples of such technologies include *inter alia* electronic funds transfer, credit and debit card transactions, use of Automated Teller Machines, telephone banking and internet banking. The following is a detailed discussion of the above named technologies:

---

[72] Association of Certified Fraud Examiners, "The Fraud Trial: The Law Against Fraud" P. 8 available at http://www.acfe.com/uploadedFiles/Shared_Content/Products/Self-Study_CPE/Fraud-Trial-2011-Chapter-Excerpt.pdf (Visited 25th September 2013).

[73] See Ravi Vadlamani, "Introduction to Banking Technology and Management." *Institute for Development and Research in Banking Technology*, IGI Global, India (2008): 1-2.

2.2.4.1 Electronic Payments

Electronic payments are effected by means of electronic instructions under which a financial institution is ordered to effect a transfer of funds.[74] Customers are for example able to pay their bills electronically by instructing their banks to debit their account and pay a third party a given amount of money.[75] The means by which payment is made varies and the two common examples are:

i. Electronic Funds Transfer (EFT)

Under this system the account holder instructs his bank to pay money to the payee's account. If the funds are available, the payer's bank debits the payer's account and pays the funds to the payee's bank, which then credits the payee's account.[76] The account holder may be having sufficient money in the account or there would be an agreed overdraft or credit facility in place.[77] EFT is an electronic fund transfer modes that operate on a Deferred Net Settlement (DNS) basis which settles transactions in batches.[78] In DNS, the settlement takes place at a particular point of time. All transactions are held up till that time. For example, EFT settlement takes place once a day. Any transaction initiated after a designated settlement time would have to wait till the next designated settlement time.[79]

ii. Real Time Gross Settlement (RTGS)

This system operates the same way as EFT by effecting transfer of money from the payer's account to the payee. However unlike EFT, RTGS transactions are processed continuously without netting (i.e they are not processed in batches).[80] RTGS system is defined as a gross settlement system in which both processing and final settlement of

---

[74] Olujoke Akindemowo, "The Fading Rustle, Chink and Jingle: Electronic Value and the Concept of Money" *University of New South Wales Law Journal* 21 no. 2 (1998): 466 ,475.

[75] Beatty Andrea; Aubrey Mark; Bollen Rhys "E-Payments and Australian Regulation" *University of New South Wales Law Journal* 21 no.2 (1998) : 489, 492.

[76] Bollen Rhys, "The Development and Legal Nature of Payment Facilities." *Murdoch University Electronic Journal of Law*, 11 no. 2 (2004): 31.

[77] Bollen Rhys, "What a Payment is and How it Continues to Confuse Lawyers." *Murdoch University Electronic Journal of Law*, (2005): 22.

[78] http://www.centralbank.go.ke/index.php/2012-09-21-11-44-41/kepss (Visited 27th September 2013).

[79] http://www.centralbank.go.ke/index.php/2012-09-21-11-44-41/kepss (Visited 27th September 2013).

[80] http://www.centralbank.go.ke/index.php/kenya-payments-and-settlements (Visited 27th September 2013).

funds transfer instructions take place continuously (i.e. in real time) from one bank to another.[81] In Kenya, the Central Bank of Kenya operates Kenya Electronic Payment and Settlement System (KEPSS) which was commissioned on 29th July 2005[82]. KEPSS is a Real Time Gross Settlement (RTGS) System. KEPSS has helped in phasing out the previous paper based inter-bank settlement system leading to efficient funds management.[83]

2.2.4.2 Credit and Debit Cards

Credit and debit cards are electronic payment instruments issued by the bank at the request of an account holder. Such cards are evidence that the card holder is a party to an existing financial relationship with the named bank[84]. The holder of such card is able to purchase goods and services without the use of liquid cash. The card holder does so by producing the physical card and inputting the PIN number.[85] The trader then processes the transaction electronically and afterwards the cardholder signs the sales voucher containing the amount which has been debited in his account.[86]

At times it may not be possible to convincingly ascertain the legitimacy of the cardholder since some cards and other means of identification may be stolen or processed through illegal means. This can lead to unauthorized transaction on a credit card or debit card account. In addition, an account holder is only able to see the transactions via the payment card only after they have received the account statement from the bank. Consequently, one may fail to detect and stop unauthorized transaction as soon as they happen.

---

[81] *Ibid.*
[82] http://www.centralbank.go.ke/index.php/kepss (Visited 26th September, 2013).
[83] http://www.centralbank.go.ke/index.php/2012-09-21-11-44-41/kepss (Visited 27th September 2013).
[84] Olujoke Akindemowo, "The Fading Rustle, Chink and Jingle: Electronic Value and the Concept of Money "*University of New South Wales Law Journal* 21 no.2 (1998): 466,474.
[85] *Ibid.*
[86] Tucker Greg, "Electronic Payment System: Some Legal Issues." *Law Institute Journal* (1997): 29.

2.2.4.3 Other Banking Transactions

Customers transact with their banks through various ways such as use of Automated Teller Machine (ATM) to withdraw cash and use of telephone banking. These are discussed briefly hereunder:

i. Automated Teller Machine (ATM)

ATMs' are operated through use of ATM cards which are authenticated by input of Personal Identification Number (PIN). Sometimes fraudulent cash withdrawals may be made from an ATM despite the fact that the card has at all times remained in possession of the cardholder.[87] This shows that such cards are prone to forgery and the fraudsters may be able to obtain account holders PIN's through various ways which are discussed in the next topic.

ii. Telephone Banking

By telephone banking customers are able to give instructions and receive information by speaking to a bank staff over telephone.[88] In order to verify the authenticity of the caller customers are asked security questions which they themselves are likely to possess. Such questions include date when the account was opened, telephone number, spouse name among other confidential information.[89] This mode of banking is likely to be abused by fraudsters by way of intercepting such conversation and as a result gaining confidential information of a particular customer. In other cases bank employees may collude with fraudsters and divulge confidential information to fraudsters who then use this information to transact by way of telephone banking and issue instructions which are detrimental to the genuine account holder.

---

[87]Bohm Nicholas, Brown Ian, Gladman Brian "Electronic Commerce: Who carries the Risk of Fraud?" *Journal of Information, Law and Technology*, 3, (2000): 10.

[88] This method of banking is only available to those customers who have made prior arrangement with their banks on the need to transact through telephone. This was clarified at an interview with a Kenya Commercial Bank employee who requested to remain anonymous.

[89] Olujoke Akindemowo, "The Fading Rustle, Chink and Jingle: Electronic Value and the Concept of Money "*University of New South Wales Law Journal* 21 no.2 (1998): 466,474.

2.3 FORMS OF ELECTRONIC BANKING FRAUD

Electronic banking fraud manifests itself in different forms. This section discusses various manifestations of electronic banking fraud though many of them overlap.

2.3.1 Identity Fraud

Identity fraud means to obtain, to possess or to create intentionally, and unlawfully or without consent false means of identification in order to commit unlawful behaviour, or to have the intention to commit unlawful behavior.[90] Identity fraud can also be as a result of identity theft, identity delegation, swapping of identities or creating a fictititous identity.[91] By falsifying an identity a person is able to gain money, goods, services or their worth through the use of false identity.[92]

Identity fraud arises when a person pretends to be someone else in order to obtain goods and services through the use of a totally fictitious name or the adoption of a real person's name either alive or dead with or without their permission.[93] Identity fraud is a tool used to facilitate commission of other crimes.[94] In a nutshell, identity fraud involves a fraudster using a victim's personal information such as name, address, bank account number, credit card details among other possible information in order to obtain an advantage[95] possibly financial benefit. Consequently identity bank fraud may manifest itself in various techniques including:

---

[90] Bald de Vries, Jet Tigchelaar & Tina van der Linden "Describing Identity Fraud: Towards a Common Definition." *Scripted* 5 (2008): 482, 495.

[91] *Ibid* p. 486.

[92] See Farrar, H John, "Fighting Identity Crime." *Bond Law Review*, 23 (2011): 91.

[93] Bald de Vries, Jet Tigchelaar & Tina van der Linden "Describing Identity Fraud: Towards a Common Definition." *Scripted* 5 (2008): 488. Adoption of a real person's name is sometimes referred to as a hijacked identity.

[94] Henry Pontell, "Identity Fraud, Cyber Crime and White Collar Delinquency", *Adelaide Law Review* 23 (2002):305, 305.

[95] Some authors have attempted to distinguish the crime of identity theft from that of identity fraud with the main distinguishing factor being identity fraud must be precipitated by the need to have material gain. Identity theft however may not necessarily result in any material gain. See Stewart Jeremy Doughlas, "South Australian Laws Target Identity Theft." *Privacy Law and Policy Reporter* 8, (2004): 4.

2.3.1.1Phishing

The internet plays a major role in the growth of identity fraud mainly due to the possibility of remaining anonymous, the availability of wide and diverse materials therein and the technological advances.[96] Phishing is an online malicious activity aimed at gaining individual's personal identity, data and other crucial information.[97] The fraudsters are able to obtain such information by enticing people into visiting fraudulent websites which they have created and persuading them to enter identity information such as usernames, personal identification numbers, addresses, social security numbers and anything else that can be made to appear credible.

The fraudsters begin this process by sending a large number of spam[98] emails which have links to those fraudulent websites.[99] The fraudulent websites are created in the name of an existing bank so that victims are led to believe that those are genuine communications.[100] Once the victim clicks on the link they are presented with accurate imitation of the legitimate bank's pages and once reassured will proceed to fill in personal details as requested.[101] Once this confidential data is obtained the fraudsters are able to impersonate the victim and access their bank accounts and either withdraw from it, apply for credit cards, take out loans in their name or do any other possible action.[102] Sometimes the said emails may be directed only to a specific victim and not any group of unsuspecting people. This is called spear phishing. An example of this is where a person may

---

[96] Pontell Henry, Identity Fraud, "Cyber-Crime, and White- Collar Delinquency" *Adelaide Law Review* 23, (2002): 35, 307.

[97] Anne Savirimuthu and Joseph Savirimuthu, "Identity Theft and System Theory: The Fraud Act 2006 in Perspective," *Scripted*,4, (2007): 436, 439.

[98] Spam is unsolicited communication, meaning that there is no prior relationship between the sender and the recipient and that the recipient has not consented to receive the communication. See Reinhardt Buys, *Online Consumer Protection and Spam* p.160 published in Reinhardt Buys & Francis buys, *Cyberlaw, The Law of Internet in South Africa*, Van Schaik Publishers (2004). In this era of mobile banking spam includes unwanted communication by way of phone that is SMS.

[99] Reinhardt Buys, *Online Consumer Protection and Spam p.160 published in Reinhardt Buys & Francis buys, Cyberlaw, The Law of Internet in South Africa,* Van Schaik Publishers (2004).

[100] Bald de Vries, Jet Tigchelaar & Tina van der Linden "Describing Identity Fraud: Towards a Common Definition." *Scripted* 5 (2008): 440.

[101] Moore Tyler and Clayton Richard, "Examining the Impact of Website Take-down on Phishing." p.2, available at http://lyle.smu.edu/~tylerm/ecrime07.pdf (visited 22nd September 2013).

[102]See Farrar, H John. "Fighting Identity Crime." *Bond Law Review Article 23,* no.1 (2011): 91.

impersonate a bank's employee and send email to a 'colleague' requesting for passwords or user name.[103] Through this a fraudster may be able to access the bank's computer system and defraud the bank through various means for example transferring money from one account to another.

2.3.1.2 Vishing

Vishing unlike phishing is the practice of using phones to steal identities and often persuading the victim to reveal confidential information. The telephone caller purports to be a bank or credit card company requesting for the victim's personal information by alleging the need to ensure account security.[104] The fraudsters may also send an email disguised as from a legitimate bank which asks the recipient to call a given telephone number. Once the recipient acts on it, the fraudsters entice the victim to give out personal information.[105] The information obtained is then used to defraud the customer. This can be by way of making a counterfeit payment cards containing the personal details of the victim. Once a fraudster has such a card they are able to enjoy the services of such a card for example shopping as if they were the legitimate owner.

2.3.1.3 Skimming

Skimming is a process where genuine data on a card's magnetic stripe such as credit and debit card or even ATM's card is electronically copied onto another.[106] Skimming manifests itself in many forms, one being where a small electronic device is inserted on a card slot of an automated teller machine which reads the magnetic strip as the user passes their card through it.[107] Such electronic devices are able to capture the user's Personal Identification Numbers (PIN) when the cardholder is using the machine. Once the

---

[103] New Zealand Law Commission, "Review of the Privacy Act." *NZLC*, 17, (2010): 446.
[104] *Ibid.*
[105] New Zealand Law Commission, "Review of the Privacy Act." *NZLC*, 17, (2010): 446.
[106] Bhatla Tej Paul, Prabhu Vikram & Dua Amita, "Understanding Credit Card Fraud." *Card Business Review*, (2003): 5.
[107] Sullivan Richard, "The Changing Nature of U.S Card Payment Fraud: Industry and Public Policy Option." 2nd *Quarter Economic Review Federal Reserve Bank of Kansas City*, (2010):101, 104.

fraudsters know the PIN number of the victim they can forthwith make a counterfeit card and use it to withdraw money from the victim's account.

At other time cashiers or employees of business establishments that accept payment cards such as credit or debit cards as mode of payment may have skimming devices with electro-magnetic stripe readers which are able to capture the details of the customer card when swiped. Such devices transfers' data from the customers' cards into blank cards.[108] These devices are often used with a camera to read the user's pin at the machines.[109] The fraudsters may thereafter use the fake card to purchase goods and services as if they were the account holder.

2.3.2 Payment Card Fraud

Payment card fraud occurs when a person gains financial or material advantage by use of a payment instrument, to complete a transaction that is not authorized by the legitimate account holder.[110] Payment instrument includes any instrument, whether tangible or intangible, that enables a person to obtain money, goods or services, or to otherwise make payment.[111] Examples of payment instruments include debit and credit cards, ATM cards, cheques or even electronic system like Real Time Gross Settlement, electronic funds transfer among others. Payment card fraud is however limited to fraud that occurs by means of usage of a tangible payment instrument such as debit cards and not payment effected through electronic means.

Fraudsters exploit the victim's personal information in their possession in order to commit this kind of fraud. The relevant personal information may include knowing for example the account number of the identified victim. They voluntarily share the account

---

[108] Stewart Jeremy Douglas, "South Australian Laws target Identity Theft." *Privacy Law and Policy Reporter*, 8, (2004):3.

[109] Bhatla Tej Paul, Prabhu Vikram & Dua Amita, "Understanding Creidt Card Fraud." *Card Business Review*, (2003):5.

[110] Brian F Caminer, "Credit Card Fraud, the Neglected Crime." *Journal of Criminal Law and Criminology*76 , no.3 (1985): 746, 747.

[111] Section 2 of the National Payment System Act, Act No. 39 of 2011.

details with them or through other ways such as colluding with bank employees who gives them certain account numbers of specified victims. Once they get the account number they emboss it on plain piece of plastic. The plastic cards embossed with the account number are then used to purchase goods and services. This is called white plastic scheme.[112]

At other times fraudsters print counterfeits cards with actual credit card numbers that they may have obtained in a variety of ways including from carbons of credit card purchase receipts.[113] Fraudsters may also use the acquired customer information to contact the bank in the name of a genuine cardholder asking that mail be directed to a new address. They also report the original card as stolen and ask for a replacement through the newly acquired address. This is called account takeovers.[114]

2.3.3 Hacking

Hacking is arguably the most prevalent form of electronic banking fraud.[115] Hacking is a general term that encompasses several activities which are offences on themselves and are facilitated through use of computers. Examples of such offences include: unauthorized access of a computer system to gain certain information; access to a computer system whether with authority or not and destroying data held therein or preventing access to such data; spreading computer viruses and such other related offences.[116] In a nutshell, hacking is the act of gaining unauthorized access to a computer system.[117]

---

[112] Caminer Brian F, "Credit Card Fraud, the Neglected Crime." *Journal of Criminal Law and Criminology* 76, no.3 (1985): 746, 752.

[113] Richard Sullivan, "The Changing Nature of U.S Card Payment Fraud: Industry and Public Policy Options," *2nd Quarter Economic Review Federal Reserve Bank of Kansas City*, (2010): 105.

[114] Tej Paul, Vikram Prabhu & Amita Dua, "Understanding Credit Card Fraud." *Card Business Review*, (2003): 4

[115] Serianu Cyber Intelligence Team, *Kenya Cyber Security Report 2012, Getting Back to the Basics*, Ed 1, (2012) P 17, online at http://www.serianu.com/downloads/KenyaCyberSecurityReport2012.pdf (Visited 28th June 2014).

[116] Loundy David J, "Computer Information Systems Law And System Operator Liability Revisited", 3 (1) *Murdoch University Electronic Journal of Law*,18 (1994).

[117] Brenner Susan W, "Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law." *Murdoch University Electronic Journal of Law* 8, no. 2 (2001): 11.

The access may have been authorized in the first place like in the case of bank employees however it becomes an offense if the access is with the intention of committing a crime. The fraudster may for example access confidential data held in the computer system and use it to gain financial advantage. For example the hackers may modify or delete data held in the computer system after gaining unauthorized access.[118] A fraudster may for example hack into the computer system of a bank, alter the account details of a given account so that any money deposited into that account is in actual sense credited in an account which the fraudster has control. The fraudsters hack into the accounts of customers or the bank's online system and they can use the access for several fraudulent activities. The fraudsters may do this for a very long time without being discovered.[119] For instance, they may just be deducting 'negligible amounts' from several accounts and if due care is not taken, it may go undiscovered.

2.4 NATURE OF ELECTRONIC BANKING FRAUD

Electronic banking fraud just like any general banking fraud may be categorized into three broad areas. The classification herein is mainly dependent on who the perpetrator is or the place of the person perpetrating or aiding in the commission of the fraud.

2.4.1 Internal Fraud

This fraud is committed against the bank or customer by the bank insiders namely management, employees or agents. An insider may take advantage of the information in their possession. For example, certain insiders may have exclusive access to accounts payables or suspense accounts which are used to record items such as loans process, money transfers or currency in transit. This makes it easier for an insider to move funds between accounts. For example an insider can create a fake account in the system and

[118] Mcleod Dane, "Regulating Damage on The Internet: A Tortious Approach?" *Monash University Law Review* 27, (2001): 346, 358.
[119] *Ibid.*

issue payment to it.[120] Another example is where a cashier receives a deposit over the counter but instead of recording the transaction in the books the cashier destroys that voucher and uses the deposit for personal use.[121]

2.4.2 External Fraud

This fraud is perpetrated by outsiders such as customers or members of the public without any assistance from bank insiders. This may take various manifestations, for example hacking into the computer system of a given bank and accessing money from a particular account. It may also take the form of identity fraud. For example, a person may steal identification documents of a given customer together with the account details. The fraudster may then be able to withdraw money from the customer's account or apply for other banking services such as credit cards, loans or even seek replacement of an ATM card.[122] A customer may also commit fraud by using legitimate cheque leafs as a bankers cheque by stamping the cheque leaf with a forged stamp so that the cheque may appear as a bankers cheque. Such a cheque may be used to defraud unsuspecting members of the public who accepts it without knowing that it is a personal cheque and the customer may not even be having sufficient money in the account.

2.4.3 Collusion Fraud

This is fraud committed through the joint effort of an insider and an outsider. An outsider can either be a bank customer or a third party.[123] Examples of collusion fraud may be instances when a bank employee divulges confidential details of an account holder to an outsider with the aim of assisting in commission of fraud. The outsider can subsequently forge identification documents of a customer and be able to take control of a customer's account by for example applying for a new PIN. Subsequently such a person is able to

---

[120] Tom Leuchtner,*4 Internal Fraud and how to Spot Them,* online at http://www.ababj.com/briefing/4-internal-frauds-and-how-to-spot-them-1965.html (Visited 16th July 2013).

[121] Egbune Okwute , "*Fraud and Forgery in the Nigerian Banking Industry: A Case Study of Staff Involvement* ", (Ahmadu Bello Univeristy Zaria, Dept of Business Administration 1995) P. 21.

[122] An interview with a KCB forensic unit bank employee(anonymous) showed that such cases are rather common.

[123] Ikechu Kanu Success & Okay Okorafor, "The Nature Extent and economic Impact of Fraud on Bank Deposit in Nigeria" *Interdisciplinary Journal of Contemporary Research in Business 4,* no. 10 (2013): 253, 256.

withdraw money from the customer's account. The outsider may also apply for credit facility or credit cards in the name of an account holder.

2.5 MEASURES TO COMBAT ELECTRONIC BANKING FRAUD

My study acknowledges that law alone cannot eradicate electronic baking fraud. Consequently banks play a big role in prevention or deterring electronic banking fraud through adoption of various relevant measures necessary to fight such fraud. Some of these measures includes: ensuring that there is a password verification page especially for customers who transact through internet banking.[124] This ensures that the customer is first asked certain confidential information to ascertain their identification before one can safely login.

There is also use of biometric enabled ATM's whereby a scanner is put in the ATM machine and when a customer places her finger in the scanner, the image is sent to the bank's main machine which confirms the identity of the user by comparing the scanned image with the stored image.[125] Access therefore is only granted when the scanned information matches the one stored by the bank. This greatly reduces instances of fraud since unlike a password which can be hacked, one's fingerprint or any biometric identity is unique and therefore hard to imitate.

Banks in Kenya have most recently also converted the debit and credit cards that have been using magnetic strip technology to chip card technology whereby built-in

---

[124] Fighting Banking Fraud without Driving Away Customers, online at https://www.iovation.com/images/uploads/white-papers/PDF/iovation-fighting-banking-fraud-white-paper.pdf(visited on 18th June 2014).

[125] White Paper, *Biometrics in Banking*, online at http://www.google.co.ke/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCkQFjAA&url=http%3A%2F%2Fwww.digitalpersona.com%2Fbiometrics-in-banking%2F&ei=9pGhU7aFI8ey0QXp24DoDQ&usg=AFQjCNFTOJHZ1ecdz4a3tMlEHPxe5Pd_YQ&bvm=bv.69137298,d.bGQ (visited on 18th June 2014).

microchips are encrypted making it difficult to counterfeit.[126] Cards that use the magnetic strip technology are prone to attacks by fraudsters since a device can easily read the magnetic strip as the user uses it hence copying the personal information which can be used by the fraudster to make a counterfeit card and use it to defraud the customer.

Other notable measures that are in use by the banks to combat electronic banking fraud or fraud generally includes: credit and debit cards alerts whereby the bank automatically notifies the customer through a short message in the mobile phone or an email anytime a transaction is made on the customer's account; the banks have also pegged the maximum amount of withdrawal which a customer can make at any given time, this ensures that a fraudster is not able to withdraw a substantial amount in the customer's account at any given time; finally the banks also ensures that a customer can regularly change their password to strengthen security of their accounts.

2.6 CONCLUSION

This chapter has discussed the nature of fraud both as a crime and as a civil wrong. Though the word fraud has no definite meaning, it has some common elements and characteristics which when read together can be said to constitute fraud. Generally, a person may seek remedy for fraud under either the criminal law or the civil law or both. This is because the offences which constitute fraud share common characteristics which are both civil and criminal in nature.

Electronic banking fraud is the fraud that is perpetrated through the use of various banking technology. This chapter has discussed the various forms of electronic banking fraud and various ways through which such fraud manifests itself. This chapter therefore, provides the basis for the next chapter which will explore the existing legal regime that

---

[126] Milcah Kwambukha, Kenya Bankers Set Deadline for Chip and Pin Tech, Web Africa Published on 8th April 2013 online at http://www.itwebafrica.com/ict-and-governance/256-kenya/230841-kenya-bankers-set-deadline-for-chip-and-pin-tech (visited on 18th June 2014).

attempt to combat such electronic banking fraud. The chapter further highlights some of the measures adopted by the banks to fight electronic banking fraud.

CHAPTER THREE

LEGAL AND INSTITUTIONAL FRAMEWORK ADDRESSING ELECTRONIC BANKING FRAUD IN KENYA

3.1 INTRODUCTION

This chapter analyses the existing Kenyan legal and institutional framework that attempts to address electronic banking fraud. The study examines relevant Kenyan statutes and subsidiary legislation. In particular, the study analyses the Penal Code, the Kenya Information and Communications Act, the Banking Act and the Central Bank of Kenya Prudential guideline. The study also discusses various aspects in which the law of tort may be relevant in combating electronic banking fraud. The chapter conducts an in depth analysis of the applicable legal provisions citing their respective strengths and weaknesses. This chapter also scrutinizes whether the stated law has kept pace with offences brought about by modern technology or whether the law is flexible enough to be applied to new situations especially brought about by technology.

Additionally, this chapter also highlights how United Nations Commission on International Trade Law Model Law on Electronic Commerce may be applied to promote global electronic commerce by encouraging legislating on relevant laws which recognizes the use of modern technology in place of the traditional paper based system. The chapter also takes cognizance of the role played by the relevant institutions tasked with investigation of fraud in Kenya. By doing so, this chapter identifies any shortcomings and or strength in the named institutions with an aim of making recommendations thereunder.

3.2 PENAL CODE

The Penal Code[127] is the main statute in Kenya that outlines various crimes and their respective penalties. Approximately 80% of the crime of banking fraud in Kenya is

[127] Chapter 63 of the Laws of Kenya.

prosecuting through the Penal Code.[128]The Code has various elaborate provisions applicable when prosecuting offences that may be said to have elements of fraud.[129] There is no definition of the word fraud in the Penal Code. Indeed there is no offence called fraud *per se*. Fraud is usually deciphered from the process of committing a crime and generally what may be initial is the fraudulent intention or fraudulent practices.

Indeed Arlidge and Parry correctly stated that:

> "... Criminal fraud generally consists in the dishonest obtaining of financial benefits at the expense of others, either surreptitiously or by means of deception. Financial benefits come in various forms, and the appropriate head of criminal liability (if any) depend on the type of benefit obtained as well as the means employed to obtain it."[130]

This phrase emphasizes what has already been stated above that in order to find out whether there has been an occurrence of fraud it may be imperative to look at the means used in achieving the end result. Fraud is mainly manifested in the actions of the offender or the means used to accomplish a certain end result. For example, deceiving someone in order to gain financial advantage. The act of deception may amount to fraudulent practices or show fraudulent intention depending with the circumstances of the case.

The Penal Code contains a number of provisions through which a person may be charged with on commission of an electronic banking fraud. Most of the offences are not only applicable to electronic banking fraud but also in many other ordinary scenarios as the case may be. For example a person may be charged with theft, obtaining by false pretense, forgery, conspiracy to defraud among others.

---

[128] This came into the limelight during an interview with an officer holding the position of a Senior Inspector at the Central Bank, Anti-Fraud Unit (a department within the Criminal Investigation Department). The interview was conducted on 13th September 2013. This could be attributed to the fact that the offences under the Penal Code are broad enough to accommodate many general crimes and also the fact that the offences therein are easier to prove in comparison to the offences in relation to computers as contained in the Kenya Information Communication (Amendment) Act of 2009.

[129] There is no offence called fraud *per se*, fraud is usually deciphered from the process of committing a crime and in essence what may be outright is the fraudulent intention or fraudulent practices.

[130] Alridge Anthony & Milne Alexander, *Alridge & Parry on Fraud*, (Sweet & Maxwell 3rd Ed 2007) para 3.02 cited in D Kebbell, "Criminal Law: Theft and Fraud." 10 *Otago Law Review* (2001): 119, 119.

This study shall analyze various applicable provisions with the aim of establishing their relevance in addressing the crime of electronic banking fraud. This part shall also scrutinize some of the subsequent amendments made thereof with an aim of establishing whether indeed they have kept pace with the modern day crimes especially brought about by technology. The study shall conclude by assessing the applicability of the given provisions in deterring the commission of electronic banking fraud

3.2.1 Theft

Section 268(1) of the Penal Code defines stealing in the following words, "a person who *fraudulently* and without claim of right takes anything capable of being stolen, or fraudulently converts to the use of any person, other than the general or special owner thereof, any property, is said to steal that thing or property."(Emphasis added). The ingredients of the offence of theft in this case are: fraudulently taking anything capable of being stolen and fraudulently converting any property.

3.2.1.1. Meaning of fraudulent intention

Fraud contemplated herein is the *mens rea.* Section 267(2) shows a number of intentions which if in existence may be used to deduce the existence of fraud. These are, *inter alia*:

(a) an intent to permanently deprive the general or special owner of the thing of it;
(b) an intent to use the thing as a pledge or security;
(c) ....
(d) an intent to deal with it in such a manner that it cannot be returned in the condition in which it was at the time of the taking or conversion;
(e) ...

Of relevance here is the intention to permanently deprive the owner of the thing stolen. In essence, the thing stolen must have initially belonged to someone else and the person stealing must have taken it without intention of returning it to the owner or once the thing is taken it would be impossible to return it in its original position.

In the case of *Williams*,[131] the English Court of Criminal Appeal sought to inject meaning into the word "fraudulently" in section 1(1) of the Larceny Act, 1916.[132] Lord Goddard CJ held thus:

> "The court thinks that the word 'fraudulently' does add, and is intended to add, something to the words 'without a claim of right' and that it means *...that the taking must be intentional and deliberate, that is to say, without mistake*. The person who takes the property must know when he takes it that it is the property of another person, and he must take it deliberately, not by mistake, and with an intention to deprive the person from whom it is taken, of the property in it. *...We think that the word 'fraudulently' in section 1 must mean that the taking is done intentionally, under no mistake and with knowledge that the thing taken is the property of another person.*" (Emphasis added)

Hence in order to show that something was done fraudulently all a person needs to show is that the alleged offender intentionally took away property knowing well that it belongs to someone else. That the defendant was not in any way mistaken as to the ownership and he intended to deprive the owner of its possession by the very act of taking it away. In essence he had no intention of giving it back to the owner at least in the condition in which it was taken.

3.2.1.2. Meaning of Things Capable of Being Stolen

Ordinarily banking fraud ultimately involves the theft of money held in an account belonging to someone else. Before the money is stolen, several other medium necessary in facilitating such theft may also be stolen in the process. For example one may steal an Automated Teller Machine (ATM) card or a payment card and use it to misappropriate the money held in a person's account. The question that arises therefore is what offence will such a person be charged with? Is it the theft of an ATM card or money?

A thing capable of being stolen must have physical substance hence a chose in action cannot be stolen.[133] In *Papua New Guinea Reg* v *Jamieson*[134] Prentice J., in a case of

---

[131] (1953)1 QB 660 (CCA), Section 1(1) states, "A person steals who, without the consent of the owner, fraudulently and without a claim of right made in good faith, takes and carries away anything capable of being stolen with intent, at the time of such taking, permanently to deprive the owner thereof...".

[132] This section is similar to section 268 which describes the offence of stealing.

stealing under a similar provision stated that if money is paid into a bank, that money becomes at once the money of the banker, as the relationship between banker and customer is that of debtor and creditor, and all that the customer has is a chose in action, that is the right to recover from the bank the amount standing to his credit.

This reasoning emanates from the fact that the relationship between a customer and a bank is a credit relationship. The account holder has a claim not to the money held by the bank but a chose in action. This is because the customer has that right to be paid on demand not the specific money deposited but a sum equivalent.

Hence a payment card can be stolen as a piece of card however the proceeds from cashing it thereof are incapable of being stolen. In *R v Wilkinson*[135] the New Zealand Court of Appeal held that, electronic transfer of funds from one person to another did not involve transfer of property and it does not involve transfer of anything that can be said to be movable. Consequently one cannot be said to obtain anything capable of being stolen. A similar decision had been reached by the House of Lords in the case of *R v preddy.*[136] This case held that electronic funds do not pass from one person to another hence cannot be said to be property belonging to someone else.

Other crucial things that may be stolen includes, confidential information held by the bank. The question then is whether information is capable of being stolen. It was held in the case of *Oxford v Moss* that a dishonest obtaining of confidential information is not theft.[137] This seems to have been the law in Kenya before 2009 when section 267 was amended to include information as a thing capable of being stolen. Consequently information was added as something that is capable of being stolen. To this extent a fraudster who hacks into a computer system and accesses confidential information of customers may, in the absence of any other relevant law be prosecuted for theft of such

---

[133] Kasaipwalova v The State (1977) PNGLR 257.
[134] (1975) P.N.G.L.R. 216.
[135] (1999)1 NZLR 403.
[136] (1996) AC 815.
[137] (1979) 68 Cr App R 183.

information. This ensures that a person may not go free even where they have committed .an offence for lack of relevant law under which to convict.

3.2.1.3. Intention to Permanently Deprive the Owner

Crimes committed through the means of technology do not necessarily involve the actual taking away of 'property.' For example the offender may copy a computer software or information stored in the computer without necessarily depriving the owner of the same information. This is not theft in actual sense since the owner still has possession and use of the information. This kind of scenario poses some problems in the application of the traditional offenses to technological induced crimes.

What offence therefore can a person be charged with if he transfers money from one account to another? Theft involves fraudulently taking anything capable of being stolen. It is fraudulent if there is intention to permanently deprive the owner of that thing. Anything capable of being stolen has been defined under section 267 as property of another which is movable or capable of being movable.

Property includes any description of movable or immovable property, money, debts and legacies, and all deeds and instruments relating to or evidencing the title or right to any property, or giving a right to recover or receive any money or goods, and also includes not only such property as has been originally in the possession or under the control of any person, but also any property into or for which the same has been converted or exchanged, and anything acquired by such conversion or exchange, whether immediately or otherwise.[138]

Indeed money, debts etc are examples of property. But do they qualify as "property of another' so that it can be said that the owner has been permanently deprived of it. The House of Lords in the case of *R v preddy*[139] stated that, effecting an electronic transfer of funds does not amount to obtaining property 'belonging to another' since the property

[138] Section 2 of the Penal Code.
[139] (1996) AC 815.

which the appellants has acquired is a new chose in action constituted by the debt then owed to him by his bank and represented by the credit entry in his own bank account. In essence, the property which the appellants acquired cannot be identified with the property which the lending[140] institution lost when its account was debited.

To this extent it is not possible to permanently deprive someone of money held in an account since it cannot be said to belong to a particular person. Each transfer of money brings with it a new proprietary interest in the form of a different chose in action.

3.2.1.4. Conclusion

The offence of theft is relevant in prosecuting banking fraud cases. However many electronic fraud cases involves theft of intangible assets which do not fall within the purview of the traditional definition of the word property. For example money held in an account is not property within the meaning of section 2 of the Penal Code. Additionally, fraud in banks may also involve stealing of confidential data held in computer system without necessarily depriving the bank of such data.[141] The offence of theft superimposes the act of permanently depriving the owner of the thing stolen and hence a fraudster in this case may easily escape liability. To this extent the offence of theft need to be amended so in some circumstances, the owner need not necessarily be *permanently* deprived of the thing stolen.

This section is also inadequate in terms of prohibiting electronic banking fraud which ultimately involves loss of money held in a particular account. For example a person may only be charged with stealing of a plastic card or a cheque leaf but not stealing of some specific money held in a customer's account since money held in an account is not considered as property but a chose in action. This therefore means that if a person forges a cheque and withdraws money from an account, such a person can only be charged with the offence of theft of a cheque leaf worthy a given amount of money mainly nominal

[140] In this case the appellants had submitted false applications to the lending institution as a result the lending institution advanced them mortgage advances. Consequently, the lending institution lost money.
[141] M. Dunning, "Some Aspects of theft of Computer Software." *Auckland University Law review*, (1978): 273, 280.

values and not the theft of the equivalent money withdrawn from that account. In essence, the value of the card or the cheque leaf does not in any way commensurate to the amount of money actually stolen.

3.2.2. Obtaining by False Pretences

Section 312 defines false pretense as any representation, made by words, writing or conduct, of a matter of fact, either past or present, which representation is false in fact, and which the person making it knows to be false or does not believe to be true. The key word here is that the person making such statements either knows them to be false or does not believe in their truth. If a person therefore makes a statement without caring to confirm their truth then such is a false pretense. Such statements are fraudulent because they cause the recipient to act in a manner in which ordinarily they would not have acted but for the lie.

Section 313 on the other hand defines obtaining by false pretense as making a false statement with intention of defrauding someone anything capable of being stolen. We have already defined on previous part what anything capable of being stolen is. Intention to defraud is an essential ingredient of this offence. So what exactly is intention to defraud?

In the case of *O'Sullivan*[142] Victoria Supreme Court said in reference to Section 409(1) of the Criminal Code of Western Australia, 1913 (similar to section 313 of the Penal Code) that:

> "..The intent to defraud includes in every case an intention on the part of the accused that the owner of the goods shall be, by such false statements, induced to do what he otherwise would not do namely, part with the goods in question."

Intention to defraud therefore arises if a person makes a false statement for purposes of inducing another to do something which they would not have ordinarily done had the statement been true. If a person therefore accesses confidential data held in a computer

[142] (1925) V.l.R. 514 , 518.

system and uses that data to create a false identity which they then use to obtain some financial advantage, then such persons can be charged with obtaining by false pretense. In essence, fraud uses deception to deprive people of their things.

This section is however insufficient in addressing electronic banking fraud because as already seen under the offence of theft there is a limitation as to something which is capable of being stolen. The problem again arises since intangible property manifesting in choses in action are not capable of being stolen. Incorporation of such in the definition of property and subsequently as things capable of being stolen would ensure that some fraudulent acts are prosecuted under obtaining by false pretense.

3.2.3 Forgery

Section 345 defines forgery as the making of a false document with intent to defraud or deceive. Through an amendment of 2009[143] section 347 introduced the element of forgery that involves:

a. fraudulently making a false document by way of transmitting or making any electronic data;
b. fraudulently, by cancellation or otherwise, altering a document or an electronic record in any material part thereof, after it has been made, executed or affixed with a digital signature either by himself or by any other person; or
c. Fraudulently, causing any person to sign, seal, execute or alter a document or an electronic record or to affix his digital signature on any electronic record knowing that such person by reason of deception practised upon him, does not know the contents of the document or electronic record or the nature of the alteration.

Electronic record in this case means a record generated in digital form by an information system which can be transmitted within an information system or from one information system to another, and stored in an information system or other medium.[144] This

[143] Act No. 1 of 2009, 6th Schedule.
[144] Section 2 of the Penal code.

amendment makes it possible to charge a person for unlawfully altering electronic data stored in a computer system. Hence if someone alters electronic data for example account details and induces another to accept the data as genuine, and because of that acceptance the genuine owner is prejudiced then such a person can be charged with forgery.

For example, a bank employee may manipulate a computer system by creating false withdrawal entries thereby stealing money from a bank. The employee may in addition to being charged with theft, also be charged with forgery. Additionally, it is also possible to charge a person for forgery incase of identity theft for example where an impostor sends an email with the aim of defrauding by forging a false identity. A person may assume a false identity by altering documents stored in the computer system or creating false documents or records and presenting them as genuine.

These amendments are sufficient in that they regulate against creating and altering electronic documents with an aim of presenting them as genuine. Electronic banking fraud ordinarily occurs through use of technology and in particular falsification or manipulation of electronic data. Consequently, by regulating against forgery of electronic records or data, the offence of forgery will play a vital role in the fight against electronic banking fraud.

3.2.4 Conspiracy to Defraud

Section 317 provides that:

> "Any person who conspires with another by deceit or any fraudulent means to affect the market price of anything publicly sold, or to defraud the public or any person, whether a particular person or not, or to extort any property from any person, is guilty of a misdemeanor and is liable to imprisonment for three years."

Lord Radcliffe stated that to defraud is to act to the prejudice of another's right namely:

> "...It may mean to cheat someone. It may mean to practise a fraud upon someone. It may mean to deprive someone by deceit of something which is regarded as belonging to him or, though not belonging to him, as due to him or his right."[145]

[145] *Welhum* [1961] AC 103, 124.

Defraud in other words means using deceitful tactics or practice to obtain something hence depriving the rightful owner of it whether or not the owner suffers economic loss. In essence, were it not for those deceitful tactics the victim would not have agreed to either part with something or do something which will be prejudicial to them.

Conspiracy on the other hand involves an agreement of two or more persons.[146] Viscount Dilhorne in the case of *Scott v the Metropolitan Police Commissioner*[147] defined the offence of conspiracy to defraud as," an agreement by two or more by dishonesty to deprive a person of something which is his or to which he is or would be or might be entitled and an agreement by two or more by dishonesty to injure some proprietary right of the victim's."

In the case of *R v Landy*[148] it was held that, " what the prosecution had to prove is a conspiracy to defraud, which is an agreement dishonestly to do something which will or may cause loss or prejudice to another." These two cases show that conspiracy exists where two or more persons are involved. Conspiracy to defraud must involve some element of dishonesty between the perpetrators.

How does dishonest occur? In the case of *R v Glenister*[149] the New South Wales court of Criminal Appeal stated that, "it is unnecessary for the trial judge to go further and define dishonesty. It is enough if he is informed the jury that in deciding whether an application was or was not dishonest they should apply the current standards of ordinary decent people."

---

[146] The Law Commission, "Criminal Law: Conspiracy to Defraud."(London 1994): 11.
[147] (1975) AC 819.
[148] (1981) 1 WLR 355,365.
[149] (1980) 2 NSWLR 597,607.

In *R v Ghosh*,[150] the court formulated some standards to determine whether the defendant acted dishonestly or not: (i) whether according to the ordinary standards of reasonable and honest people the conduct was dishonest; and (ii) if it was dishonest by those standards, whether the defendant himself must have realized that what he did was by those standards dishonest.

3.2.4.1 Applicability of Conspiracy to Defraud in Banking

Although the offence of conspiracy to defraud is quite general, when applied in the banking context, a person can be charged under it. For example, a bank employee may assist another to access confidential information of a certain customer and that information may then be used to the detriment of the customer. For example, making a counterfeit card from the information obtained therein and use it to purchase goods and services.In other cases one can obtain a loan by masquerading as the real customer. Such persons can therefore be charged with conspiracy to defraud.

The *mens rea*[151] that is relevant in this offence is to defraud the public or any person. A person here may be natural or artificial eg a company or a public body. The *actus reus*[152] is to conspire. This therefore is a crime that involves two or more persons.

3.2.5 General Appraisal

A general analysis of the relevant offences applicable in cases of fraud shows that irrespective of the nature of the fraud, a person can always be charged under the Penal Code. The use of technology may have led to the devising of various ways of committing fraud. However the offences under the Penal Code are general enough to accommodate

---

[150] (1982) QB 1053.

[151] *Mens rea* refers to the mental element of a crime. The legal dictionary defines mens rea as "As an element of criminal responsibility, a guilty mind; a guilty or wrongful purpose; a criminal intent. Guilty knowledge and wilfulness." http://legal-dictionary.thefreedictionary.com/mens+rea (Visited on 14th July 2013).

[152] This is the criminal act. The legal dictionary defines it as, "As an element of criminal responsibility, the wrongful act or omission that comprises the physical components of a crime. Criminal statutes generally require proof of both actus reus and mens rea on the part of a defendant in order to establish criminal liability." http://legal-dictionary.thefreedictionary.com/actus+reus (Visited on 17th June 2013).

various nature and manifestations of crime of fraud. The Penal code is therefore used as a safeguard against any chance of escaping liability.

The Penal Code provides for criminal sanctions in terms of fines and imprisonment. Though criminal sanctions are generally supposed to have deterrence effect the crime of fraud is still on the rise. An offence can be said to have effective deterrence effect if the penalties thereof are harsh enough to either deter the criminals or potential offenders.[153] Most of the fraud related offences under the Penal Code are treated as misdemeanors.[154] As such they attract minimal penalties hence making it unrealistic to attempt to deter offenders and potential offenders too.

For example, the offence of obtaining by false pretense, forgery and theft attracts a penalty of three years imprisonment. The three years imprisonment may not be sufficient enough depending with the kind of fraud perpetrated and the loss suffered. Additionally, even the offences that are treated as felonies, the Act provide a maximum penalty hence giving the judicial officer a wide discretion in sentencing. An example is a felony committed by a bank under Section 316B which attracts a maximum penalty of only five hundred thousand shillings. Such an amount is way too little as many banking institutions have a very high capital base and the fraud committed may have involved loss of millions of shillings.

Technology brings with it new ways of committing crime and the sophistication of crimes depends with the level of innovation. The 2009 amendments attempted to enlarge the scope of applications of fraud to include fraud perpetrated through electronic means. For example the offence forgery under section 347 was expounded to include fraudulently making or transmitting electronic records. Again section 267 which outlines

---

[153] Gray Anthony, "Criminal Sanctions for Cartel Behaviour." *Queensland University of Technology Law and Justice Journal*,8 no.2 (2008): 364, 369 See also Mohd Kassim and Bin Noor Mohamed, "Problems Faced by the Criminal Justice System in Addressing Fraud Committed by Multi national Corporations," *Internet Journal of Criminology*, 26 (2006).

[154] Misdemenours are offences that are considered as 'small offences'. Offences that are not felonies. See Section 4 of the Penal Code.

things that are capable of being stolen included the word information as a thing capable of being stolen.

The specific 2009 amendments mentioned herein were geared towards addressing crimes perpetrated through the use of technology which involves in most cases the transmission, altering, deletion or suppression of information stored in electronic gadgets. To that extent it is in order to conclude that the Penal Code has attempted to address at least in a way electronic banking fraud.

The amendments of 2004 on the other hand, and in particular the addition of section 316A and 316B which were specially meant for banking institutions did not however address electronic banking fraud. Section 316A for instance criminalizes the conduct of individuals issuing bad cheques. Section 316B on the other hand provides for circumstances when a bank may be held liable as a result of any possible fraud perpetrated through issuing of cheques and other related instruments. The offences contemplated herein are not committed through use of technology and as such are not relevant to this study.

The study concludes that generally, the amendments in the Penal code do not reflect the mutations of crime brought about by technological changes. The only attempt that has been made includes incorporating electronic transaction in the offence of forgery and including information as something capable of being stolen. These additions are insufficient in comparison with the magnitude and mutations of the crime of fraud. It is therefore necessary to update the code to bring it in line with the technological advanced crimes notably banking fraud. This is likely to reduce the vulnerability of our banking institution from being attacked by fraudsters.

3.3 THE KENYA INFORMATION AND COMMUNICATIONS ACT

This Act[155] was enacted in 1998 to establish the Communications Commission of Kenya (CCK) which is tasked with facilitating the development of *inter alia* electronic commerce. The Act was amended in 2009 thereby incorporating various technology induced crimes. The amendments seem to have been necessitated by the need to address crimes committed through use of technology namely computers and the absence of any other relevant law that attempted to address such issues. The Act was further amended through the Kenya Information and Communications (Amendment) Act, 2013.[156] The amendments replaced the CCK with the Communications Authority of Kenya (CAK). The main purpose of the amendments was to provide for an independent authority in line with the Constitution and especially with regard to media freedom as enshrined under Article 34 of the Constitution. Consequently, the amendments do not have any impact or bearing in the foregoing discussion.

The relevant provisions with regard to electronic banking fraud are contained in section 83 and 84 of the 2009 Act. Some these offences include:

3.3.1. Unauthorized Access and Interception of Computer Service

Section 83W prohibits any access to a computer system for the purpose of obtaining a computer service or to intercept any function or any data within a computer system. It is also an offence to access a computer system and thereby cause any modification, suppression or impairment[157] of data held therein. This offence may be used to prosecute hackers who by unauthorized access cause damage through modification and interference by deletion or otherwise of data held in a computer system or even interfering with the operation of a computer system.

---

[155] The Kenya Information and Communication Act, Chapter 411A of the Laws of Kenya.
[156] This was by way of the Kenya Gazette Supplement No.169A published on 18th December, 2013. The commencement date was 2nd January 2014.
[157] Section 83W(3).

Interception on the other hand includes listening to, recording a function of a computer or acquiring the substance, its meaning or purport of such function.[158] Of relevance in electronic banking would be unauthorized interception or access of electronic data. A person therefore who accesses any electronic data stored in a computer system and who uses it to commit any fraud would be liable under this section. A hacker for example may be able to bypass security system and access information stored in a computer system.[159]The act of accessing or intercepting is an offence on its own even without any subsequent use of the data so accessed.

3.3.2. Access with Intention of Committing an Offence

Section 83V prescribes the offence of accessing any program or data held in a computer system with an intention of committing an offence. What is required herewith is the prior intention to commit an offence. A person therefore who attempts to modify some data but is apprehended before completion may be charged under this provision. The offence is punishable whether the access was authorized or not.

It will still be an offence if someone actually commits the offence that they initially intended or other corresponding offences. The distinguishing factor with the earlier kind of access is one may have been authorized to gain access in the first place. This way the offence targets insiders who may have authority to access certain data or program but uses that privilege to commit an offence.

3.3.3. Unauthorized Disclosure of Password

It is an offence under section 83Z to disclose any password, access code or any means of gaining access to any program or data so held. The disclosure must be done with the intention of having any wrongful gain, disclosure for unlawful purpose or knowing the disclosure may cause any prejudice to any person. This section may be used to apprehend

---

[158] Section 2.

[159] New Zealand Law Commission, "Are Changes to the Criminal Law needed?" Para 56 online at http://www.commonlii.org/cgi-bin/disp.pl/nz/other/nzlc/report/R54/R54.3.html?stem=0&synonyms=0&query=%22altering%20a%20document%20%22 (visited 9th September 2013).

a bank employee who willfully discloses his password to another person with an aim of assisting in commission of an offence.

3.3.4. Electronic Fraud

Section 84B regulates against fraudulently causing loss of property of another person by an input, alteration, deletion or suppression of any data or any interference with a computer system. At a glance one can safely conclude that the definition captures electronic banking fraud. This is because electronic banking fraud is committed through manipulation of various banking technologies with an aim of gaining financial advantage. The manipulation could be in terms of altering, deletion, suppression or in any way interfering with any data or system.

The term "property" is however not defined in the Act. We have already identified the shortcoming of the term 'property' as defined in the Penal Code. But is money really property as envisaged in this section. In electronic banking fraud there would be in almost all instances loss of money which was previously held in a certain account. For example specifically in relation to this section, a bank employee may alter or interfere with the banking system and send instructions directing the system to debit one person's account and credit his own account. With reference to that example the question would be whether such loss of money is contemplated in the definition of electronic fraud under the Act.

The shortcoming of inclusion of money[160] as property as defined in the Penal Code is that the definition is restricted to the physical money and not the right over a chose in action. One cannot identify specific's person money once deposited but the depositor only gets a right of a chose in action in terms of an equivalent sum of money.

Prominently missing also in the Act is the definition of the term 'fraudulently'. Whereas the section regulates against fraudulently causing loss of property of another, there is no

[160] Section 2 of the penal Code defines property to include money.

really the exact meaning of this term. The Penal Code in the definition of the offence of theft defines fraudulently as the intention to permanently deprive the owner of the thing stolen. I do not think that it would be appropriate to impose that definition herein due to its already identified shortcoming. Even if we may result to common law in an attempt to deduce it's meaning, it would always be better if the drafters inserted the meaning of the term 'fraudulent' especially bearing in mind that the essence of the section was to regulate against electronic *fraud.* There is always danger in diluting the real meaning of a provision where such provision may be subject to diverse interpretation.

In conclusion, whereas this section regulates against electronic fraud, the identified shortcomings surpasses any intended benefit since the section would only take effect after interpretation by the courts in an attempt to inject meaning to it. In such cases there is always the danger of diluting the real intention of the law. Whereas it seems that the deficiency herein could be cured by way of an amendment the lingering question in this regard is whether indeed the KIC Act is the right forum to regulate against electronic fraud even generally. The main objective of the Act is to establish CCK now CAK for purposes of facilitating information communications industry. Even the 2009 amendments are mainly computer/ computer system related offences and insertion of electronic fraud ought to be seen in that light. It therefore brings in difficulties to try to harmonise the offence of electronic banking fraud with the 2009 amendments since it is clear that when the drafters were incorporating those offences, they did not have specifically the offence of electronic banking fraud in mind.

In summary the offences that can be committed under this Act are as follows:

a. Unauthorized access; this means that the mere act of accessing without permission is in itself an offence.[161]
b. Access with intent to commit an offence. Under this it is immaterial whether the access is authorized or not.[162] This section would be used to hold employees liable

[161] Section 83 U.

since in many instances they may have the right to access some data stored in a computer system, however they may take that advantage to commit offences. Another example is a hacker may access a bank's computer and transfer funds from a third party's account to another.

c. Unauthorized interception of any function or any data within a computer system.[163]

d. Unauthorized modification, suppression or impairment of any data stored in a computer system.[164]

e. Unauthorized denial of access or impairment of any data stored or program stored in a computer system.[165]

f. Unauthorized creation, publication or sharing of electronic signature certificate for fraudulent purposes.[166] This section may be applied to hold liable employees of a bank who may disclose customers' details to fraudsters and also customers who may collude with fraudsters.

3.3.5 General Appraisal

This Act has extensively regulated against misuse of computer systems and data contained therein. There is, however, need to define the meaning of the term "property" in reference to computer system and technology. This study proposes that property should incorporate those bundles of rights that arise as a result of value placed on something. Further we have also seen that even the term 'fraudulent' in relation to electronic fraud has also not been defined.

In the US the courts have attempted to define property by expounding the word to incorporate intangible property and interests. Mosk J in the Supreme Court of California said that:

---

[162] Section 83V.
[163] Section 83W.
[164] Section 83X.
[165] Section 83Y.
[166] Section 84 E.

> "The term 'property' is sufficiently comprehensive to include every species of estate, real and personal, and everything which one person can own or transfer to another. It extends to every species of right and interest capable of being enjoyed as such upon which it is practicable to place a money value.[167]"

This study recommends that the Kenya Information Communications Act should be amended to define the word property. It is proposed that property should include both tangible and intangible assets. This is because computer technology has brought with it many proprietary interests which do not normally exist in physical forms.

It is commendable to note that the Act has attempted to legislate on many aspects of computer misuse which are likely to be used by fraudsters. To that extent the Act comprehensively covers an aspect of electronic banking fraud which is the pathway of committing the offence. In essence, acts of deletion, suppression or altering electronic data or system are some of the means the fraudsters use in perpetrating electronic banking fraud.

Just like the Penal Code however, the Act provides for criminal sanctions. Consequently, it faces similar shortcoming of providing for very lenient penalties. For example any person who causes unauthorized modification of computer data is liable to a fine not exceeding KShs 500,000/= or to imprisonment for a term not exceeding three years.

Firstly the fine provided herein is way too little bearing in mind the potential loss that the fraudsters are likely to cause. The end result is that a fraudster would prefer to commit a fraud, if successful attain much money and comfortably pay the fine. In any case this is a maximum fine which an offender ought to pay. It can even be much lower depending with the circumstances of the case. Again the imprisonment period of three years that is provided herein would not deter offenders and potential offenders. Even if a person is jailed for the maximum period, they would soon leave prison and live to enjoy the fruits

[167] Dane Mcleod, "Regulating Damage on The Internet: A Tortious Approach?" *University of California Law review*, (1990): 353.

of their commission of fraud. To this extent this Act is insufficient to address the crime of electronic banking fraud.

3.4 BANKING ACT

The Banking Act[168] is the main statute that regulates banking business in Kenya.[169] The Act is not really a penal law but its objective is to regulate banks. The Act contemplates two ways of committing fraud: fraudulent practices and false accounting.

3.4.1 Fraudulent Practices

Section 11(h) of the Banking Act prohibits any institution from advancing credit, incurring liability, entering into contract or conducting its' business in a fraudulent manner. The Act describes a fraudulent conduct to include "intentional deception, false and material representation, concealment or non-disclosure of a material fact or misleading conduct, device or contrivance that results in loss and injury to the institution with an intended gain to the officer of the institution or to a customer of the institution."

This section is inadequate in two ways. Firstly, it prohibits fraudulent practices by the institution and not on the officers in those institutions. The officers therefore would escape liability even where they are personally involved in aiding perpetration of a given fraud. An argument can however be made that in as far as Section 50 of the Banking Act places a duty on every officer to ensure compliance with this Act failure to which such officers would be held liable, then on the same note an officer can be apprehended if they fail to take reasonable step to prevent commission or furtherance of fraudulent practices by an institution.

Secondly, the fraudulent conduct herein must result into loss on the part of the institution and a gain on either an officer of the bank or a customer. This is not necessarily the case as a greater percentage of banking fraud occurs even without the knowledge of the bank employees or the customer. Some of those include hacking, phishing, vishing, payment

[168] Chapter 488 Laws of Kenya.
[169] See the preamble of the Banking Act.

card fraud among others which in many cases results in no benefit to either the officers of the bank or the customer. This section therefore seeks to address only internal bank fraud or the fraud perpetrated through collusion. It is therefore insufficient in this regard.

3.4.2. False Accounting

Section 50 criminalizes the conduct of an officer who fails to take reasonable steps to ensure the accuracy and correctness of any statement submitted. The officers may commit fraud by falsification of documents or withholding some crucial information. This is because fraud involves elements of deception, concealment of non disclosure of material information.[170]Officers of a bank may be held liable for fraud where they make a false representation or withhold certain information.[171] This is an example of how internal bank fraud may occur. The bank employees may therefore be held liable where they alters some documents or fail to reveal information within their knowledge useful in curbing fraud.

3.4.3 General Appraisal

The Banking Act has in a way addressed some aspects of technology induced banking fraud. The Act criminalises the act of false accounting and fraudulent practices which have elements of fraud. Though these offences do not sufficiently address the offence of electronic banking fraud as seen above, it is commendable to note that the Banking Act has made an attempt to regulate some of these instances of the occurrence of fraud .

The Act has, in this regard, introduced criminal sanctions in terms of fine and imprisonment for offences committed thereunder. This study proposes that the sanctions provided therein should ideally commensurate to the gains made from the alleged wrong. Section 49 of the Banking Act prescribes penalty on both the institution and officers who contravene the provisions of the Act. In case of a bank corporate the fine should not

[170] Section 11 of the Banking Act.
[171] Hemming Andrew, "A Tale of Abuse of Position and False Accounting." *UNDARL*, 11,(2009) 34.

exceed one hundred thousand shillings. Individuals on the other hand are liable to a fine of not more than fifty thousand or imprisonment of not more than two years or both.

Additionally, section 50 makes it an offence for any officer of the bank to fail to take reasonable step to ensure compliance with the Act and also to fail to ensure accuracy and correctness of the financial statements submitted. The said individuals are liable to pay a fine not exceeding twenty thousand shillings or imprisonment for a term not exceeding one year or to both.

The maximum penalties prescribed herein are way too low bearing in mind the magnitude of the offence of fraud and the loss suffered. There is need for a powerful deterrence tool to the potential offenders. The study proposes a higher maximum fine which should be computed as a percentage of the loss sustained. Other studies have even suggested that the sanctions should include public condemnation in terms of media advertisements setting out details of the corporation criminal conduct and compulsory reporting to shareholders through the annual reports.[172]

In addition to the criminal sanctions provided therein, the Act also stipulate that an officer of a financial institution convicted of a crime involving fraud shall cease to hold office and shall not hold office in any other institution.[173] Fraud may affect the moral and professional unsuitability of persons proposed to be directors or senior officers of a financial institution.[174] Fraud will also disqualify one from being a member of a credit reference bureau according to rules 22 and 23 of the Banking (Credit Reference Bureau) Regulations, 2008.

These further penalties appear harsh enough to deter offenders. The offence of fraud has been isolated as a serious offence that warrants other condemnation in terms of moral suitability and inability of the offenders to hold other similar position in an institution.

---

[172] Fisse Brent,"The use of publicity as a Criminal Sanction against Business Corporations." *Melbourne University Law review,* 8 (1971): 107, 108.
[173] Section 48[1]b of the Banking Act.
[174] See section a[iv]the first schedule as read together with ss 4 and 32A of the Banking Act.

This study concludes that to this respect the penalty provided herein is sufficient to not only deter offenders but also to ensure that the bank management is alert enough to prevent or apprehend any act of fraud.

3.5 THE CENTRAL BANK OF KENYA PRUDENTIAL GUIDELINE ON FRAUD

The purpose of the guidelines is to provide information that businesses seeking to conduct the banking business in Kenya must have. The guideline provide clear guidance on the conditions applicants must fulfill to be eligible to be granted a licence to conduct banking, financial or mortgage institutions. They are drawn by the Central Bank of Kenya in pursuance of section 4 of the Central Bank of Kenya Act.[175] They are therefore binding in that the CBK is mandated to formulate and maintain monetary policy and in doing so it has to continuously issue policies and guidelines to be followed by the relevant institutions. By the fact that the guidelines are issued pursuant to the Central Bank of Kenya Act, they can be said to have attained the status of a subsidiary legislation.

The banking institutions are required to take precautions to safeguard confidentiality of customer information and transactions. The officers of the bank are supposed to maintain confidentiality of information and transactions that are within their knowledge whether during or after employment. Sometimes fraudsters collude with bank employees in order to get some crucial information necessary for the commission of fraud. At other time the employees themselves are the fraudsters since they are in a position to access the necessary details for the commission of offence. This involves the breach of their duty of confidentiality.

Fraudulent banking is one of the business activities prohibited under the Banking Act[176]. The guidelines reiterate the prohibition of fraudulent activities as stipulated under section

[175] Section 4 and 4A of the Act mandates the CBK to formulate and implement such policies as best promote the establishment, regulation and supervision of effective and effective payment, clearing and settlement systems.
[176] See section 11(1)h of the Banking Act.

11 of the Banking Act. Fraud is also listed as one of the predicate offences under the guidelines.[177]Under the guidelines, fraudulent means:

> " intentional deception, false and material representation, concealment or non-disclosure of a material fact or misleading conduct, device or contrivance that result in loss and injury to the institution with an intended gain to the officer of the institution or to a customer of the institution."

There are a number of measures under the guideline that are intended to prevent fraud. It is important to note that the Central Bank of Kenya has incorporated in the guideline measures provided for in the Basel Accord particularly the recommendations by the Electronic Banking group (EBG) of the Basel Committee on banking supervision [178] whose mandate is to develop and share sound supervisory guidance and risk management principles and enhance cross-border co-ordination among bank supervisors on e-banking activities. The EBG issued a paper on risk management principles for electronic banking in May 2001.[179] It recommended that as a basic policy banking supervisors /regulators should expect the banks to pro-actively assess various risks posed by emerging technologies and design customer identification procedures with due regards to such risks.

---

[177] A predicate offence is an offence that happens in the course of committing other offences.Other predicate offences under the guidelines are human trafficking, robbery, corruption, bribery, insider trading and counterfeiting of goods. See P. 177 of the guidelines.

[178] FSF(Financial Stability Forum) Material: Discussion papers and feedback (Archive 31/3/2013); The FSF's Approach to the regulation of e-commerce, online at http://www.lexisnexis.com/uk/legal/results/enhdocview.do?docLinkInd=true&ersKey=23_T19909269484&format=GNBFULL&startDocNo=0&resultsUrlKey=0_T19909272538&backKey=20_T19909272539&csi=280279&docNo=6 (visited 20th May 2014). This is a sub-group of the main Basel Committee and comprises 17 central banks and bank supervisory agencies from the Basel membership, along with observers representing the European Central Bank, the European Commission and the bank supervisors in Australia, Hong Kong and Singapore. It first met in November 1999.

[179]Some other relevant subsequent papers include, Bank for International Settlement, "Basel Committee on Banking Supervision, Management and Supervision of Cross-Border Electronic Banking Activities" (July 2003).

Some of the relevant measures provides for in the guidelines includes:

3.5.1 Consumer Protection and Agency Banking Measures

Banks are required to put in place measures that will protect the consumers of their services from fraud, loss of privacy or loss of service.[180] Emphasis is given to customer security with regard to agent banking.[181] Agent banking business means business carried out by an entity that has been contracted by a banking institution and approved by Central Bank to provide services of the institution on behalf of the institution.[182]

Some of the permissible banking activities through agency banking include: cash deposit and withdrawal, transfer of funds, collection of debit and credit cards, agent mobile phone banking services and cheque book collection by customers. The agents have specifically being prohibited from opening customers' accounts, granting of loans or providing cash advances.

In order to safeguard against commission of fraud, the guidelines requires that the agents should identify the customers with at least two factor authentication such as ID's, PIN's, password, ATM card, secret code or secret messages. Additionally, all electronic transactions must be in real time. Whereas these measures are necessary in curbing electronic banking fraud, agency banking is still prone to similar vulnerabilities just like the banks. These include identity theft which can occur during withdrawal of money, ATM card and cheque book collection among others.

The agents are also required to disclose to the customers in a conspicuous place a list of the banking services offered, the name of the institution it is working for, and a written notice when the electronic system is down making it impossible for the agents to transact. These and other measures ensure that the agent does not engage in unauthorized transactions without the knowledge of the customers. An agent who is proven to have had

---

[180] See Paragraphs 9.1.1 and 9.1.2 of the guideline.
[181] *Ibid.*
[182] Guideline on Agent Banking - CBK/PG/15.

criminal record involving fraud, dishonesty, integrity and other financial malpractices[183] would consequently cease to offer agency banking. The agency contract shall forthwith be terminated.[184] These guidelines if strictly followed can go a long way in reducing fraud by banks.

3.5.2 Customer Identification Measures in Electronic Banking

The guidelines embrace the fact that the growth of telephone and internet banking has provided new avenues for fraud. They therefore require any bank that is involved in these forms of banking to implement procedures to identify and authenticate the customer by ensuring sufficient communication to confirm address and personal identity.[185]

The guidelines require that the identity procedure be as robust as possible as is the case with face to face transactions.[186] Some of the specific measures are listed under paragraphs 11.11.7 and 11.11.8 of the guidelines. They include checking current utility bills of the customer, their local authority tax bill, institution statements and checking that the documents offered are original and authentic.[187] Others include checking any inconsistencies in the information given in computer systems, telephone contact with the applicant on an independently verified home or business number, checking salary details et al.[188]

Staff undertaking telephone banking are required to be sufficiently trained to enable them sufficiently identify potentially suspicious responses and guard against inadvertent disclosure of confidential information.[189] These and other measures commonly duped as "know your customer" aims at preventing occurrence of fraud and money laundering. Such measures if strictly followed would reduce instances of identity theft which may

---

[183] *Ibid.* Subsection VI. P 307.
[184] See paragraph 4.8 for factors that will lead to the termination of the agency contract.
[185] See page 191 of the guidelines.
[186] *Ibid.*
[187] See paragraph 11.11.7 of the guideline.
[188] See paragraph 11.11.8 of the guideline.
[189] Para 4.4.1.8.

occur when a fraudster assumes a false identity of a customer and presents himself as the genuine customer.

3.5.3 General Appraisal

The Central Bank of Kenya has sufficiently provided for guidelines useful in the conduct of banking business. The guideline contains relevant provisions aimed at ensuring that the banking business is conducted in a way that does not prejudice the customers as well as the banking institutions. The provisions highlighted above aimed at curbing fraud are sufficient in that they clearly stipulate mechanisms that should be followed in the conduct of business, which in the end aids in elimination of fraud. To this extent the guidelines serves a proper and vital role in eradication of electronic banking fraud in Kenya.

3.6 THE LAW OF TORT

The study has already analyzed criminal law that addresses the crime of electronic banking fraud. Criminal law however is tainted with shortcomings in terms of its insufficiency in the imposition of adequate criminal sanctions necessary to deter offenders. Could the law of tort therefore be the solution?

Electronic banking fraud occurs ordinarily as a result of unlawful interference with the computer system or data held therein thereby occasioning loss and injury. Some of the relevant tort under which a person can be prosecuted for includes:

3.6.1 Trespass and Conversion

Tort of trespass is the intentional interference of goods in possession of someone else.[190] The interference must be wrongful or intentional.[191] Acts of hacking and sending of spamming messages may be said to be conduct which interferes with someone's property. When a person hacks into a computer system, they assume control of something that belongs to another. On the other hand if unsolicited messages are sent to someone

[190] Fleming John G, *The Law of Torts* 9th ed. (North Ride: Information Services, 1998).
[191] *Penfolds Wines Pty Ltd v Elliott* (1946) 74 CLR 204, 214.

else, that amounts to unlawful interference with an email address belonging to another. This is because such messages normally appear in bulk and usually they assume space meant for other legitimate communication and to some extent they may deny the owner the chance to access and locate other relevant emails and in other cases they can even cause deletion of legitimate emails.

To be able to compensate for damage caused by hacking or transmitting of spam messages in an action for trespass, it would be necessary to conclude that such conduct is an interference with goods, that there is liability for unintentionally transmitting a virus and that intangible property can be actually damaged.[192]

Hacking is the unauthorized access to a computer system.[193] Trespass on the other hand is unlawfully gaining access to someone else property. This establishes the relationship between hacking and trespassing. In essence hacking is an example of trespass. Conversion on the other hand is the deliberate and willful dealing in a manner inconsistent with the rights of true owner[194].In *America Online v IMS*[195] unsolicited spam emails were considered to constitute actionable conversion and trespass. It was viewed as appropriating computer facilities without authorization for their own purposes. Junk email overloads the system causing malfunctions and deprives other users of legitimate use of the system.

In *Mundy v Decker*[196] an employee's deletion of email was held to constitute conversion. On appeal the issue was whether the computer directory and the individual file that were deleted had proprietary value aside from the tangible forms that could be printed. Decker's actions in deleting the entire contents of the directory were held to be wrongful

---

[192] Dane Mcleod, *Regulating Damage on the Internet: A Tortious Approach?* p. 371 http://www.austlii.edu.au/au/journals/MonashULawRw/2001/14.pdf (visited 18th September 2013).
[193] Susan W Brenner, "Cybercrime Investigation and prosecution: The Role of Penal and Procedural Law." *Murdoch University Electronic Journal of Law* 8, no. 2 (2001):10.
[194] *Ibid n.69. p.370.*
[195] 24 Fsupp 2d 548 (ED Va, 1998).
[196] 1999 WL 14479 (Unreported, Nebraska Coua of Appeal, 5 January 1999).

exercise of dominion over Mundy's property, thereby establishing a cause of action in conversion.

The court in *CompuSewe Inc. v Cyberpromotions*,[197]held that Cyberpromotions committed the tort of trespass on personal property by using CompuServe's computer system without permission. For tort of conversion and trespass to occur first of all there is need to be a general agreement showing that intangible property is capable of being converted and trespassed against.

Technological advancements have resulted in banks interacting with their customers through cyber space rather than physical interactions.[198] Today banking transactions are made through electronic records which may be processed anywhere in the world depending on the source and recipient of the relevant transactions.[199] This means that different banks irrespective of jurisdiction may have legitimate interest in the operation and regulation of a single bank account.[200]

Litigating for such crimes under tort law is advantageous in that the burden and standard of proof are much lesser than under criminal law. The banks being the main victim of banking fraud in terms of the risk of reputation loss and bearing the burden of compensating their customers for most risks have the capacity to litigate civil claims.

Tort law being a civil law will give the banking institutions the full control of the investigations. They will also be the prosecutors. The banks have sufficient machinery and capacity to investigate high level technology fraud. They have both financial capacity and human resource power. Civil remedies provided in terms of compensating for damages causes are also likely to deter offenders and potential offenders in comparison to

---

[197] 962 F Supp 1015 (SD Ohio, 1998).
[198] Chaikin David, "A Critical Examination of How Contract Law Is Used by Financial Institutions Operating in Multiple Jurisdictions." *Melbourne University Law Review* 34, no.1 (2010): 34, 38.
[199] Dimitris N Chorafas, *Electronic Funds Transfer* (Butterworths, 1988) p. 19.
[200] Chaikin David, "A Critical Examination of How Contract Law Is Used by Financial Institutions Operating in Multiple Jurisdictions." *Melbourne University Law Review* 34, no.1 (2010):34.

the criminal sanctions. This shows that the place of tort law in fighting electronic banking fraud should not be overlooked.

3.6.2 Tort of Deceit

The tort of deceit provides a civil remedy to persons who have relied on a false statement. The elements of this tort include:

(a) A representation of fact made by the fraudster;
(b) The representation must be false;
(c) It must have been made dishonestly; and
(d) It must be proved that the representation must have been intended to be relied upon and was in fact relied upon.

In the case of *Derry v Peek*[201] Lord Herschell held that:

> "First, in order to sustain *an action in deceit*, there must be proof of fraud and nothing short of that will suffice. Secondly, fraud is proved when it is shown that a false representation has been made (1) knowingly, (2) without belief in its truth, or (3) recklessly, careless whether it be true or false".(Emphasis added)

Electronic banking fraud may manifest itself in the form of tort of deceit where for instance a fraudster assumes the identity of a bank customers for example in cases of identity theft and makes a false representation to the bank official who relies on it and acts to the prejudice of the genuine customer. The impostor may for example collect a customer's ATM card without their authorization, or makes an unlawful bank transfer or does any other act prejudicial to the interests of the genuine customer. The representation by the fraudster must have been made with the intention that the receiver will be induced to act on it.

3.6.3 General Appraisal

It is a principle of tort law that a victim of fraud whether by deceit or otherwise is entitled to recover damages for the loss occasioned.[202] Civil proceedings in tort provide for the

[201] (1889) 14 App. Cas. 337.

recovery of compensatory damages or other remedies (such as injunctions), for injuries or losses caused by the acts of another in breach of a right or duty imposed by law.[203] One can therefore claim damages which commensurate with the amount of loss suffered. If a fraudster occasions loss worthy twenty million shillings, then on proof of the occurrence of such loss a victim may be compensated the amount of loss suffered. To this extent civil law would be more appropriate as deterrence tool in comparison to criminal law. This study recommends that banks and other victims of bank fraud should consider instigating civil proceedings against the offenders in contemporaneous to criminal proceedings.

3.7 UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW (UNCITRAL) MODEL LAW ON ELECTRONIC COMMERCE ("UNCITRAL MODEL LAW")

The UNCITRAL Model Law was adopted in 1996 with an aim of providing national legislators with a set of internationally accepted rules aimed at removing obstacles and increasing legal predictability for electronic commerce.[204] This Model law lays out criteria under which electronic communications may be considered equivalent to traditional paper based systems. Consequently, several countries have enacted legislation based on the Model Law. Some of those countries include, the states of Australia, Canada, Malaysia and closer home there is Ghana, Rwanda and South Africa.[205] Kenya has not yet enacted a legislation that incorporates the guiding principles as enlisted in the Model Law. Though a country is not bound to accept the guidelines stipulated in the Model Law, many countries would be ordinarily compelled to accept the internationally agreed standards and principles in order to fit in the large international community.

---

[202] S.S.P, "*Measure of Damages for Fraud and Deceit.*" Virginia Law review 47, (1961) :1209.
[203] Jane Swanton, "*The Convergence of Tort and Contract.*" Sydney Law Review, 12, (1989): 40, 45.
[204] See http://www.uncitral.org/uncitral/uncitral_texts/electronic_commerce/1996Model.html (Visited 26th October 2013).
[205] http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html (Visited 26th October 2013). The list provided in the UNICITRAL websites only contains the names of the countries whose enactments were made known to the UNICITRAL Secretariat.

Some of the relevant provisions provided for in the Model Law include:

3.7.1 Definition of the term 'Commercial'

The Model Law suggests that the term 'commercial' should be given a wider interpretation so as to cover matters arising from all relationship of commercial nature. This would include banking, insurance and construction of works among others. This definition takes cognizance of the fact that with the increase in the use of technology many transactions are now moving from the traditional paper passed mode of transacting to electronic. Commercial in this sense does not only involve the traditional meaning of buying and selling but any relationship that exist between two parties with one party offering a service etc and the other receiving that service. In banking for example, this includes, offering of loans, advances and other related products.

3.7.2 Legal Recognition of Data Messages

The Model Law also suggests legal recognition of data messages. Data message means information generated, sent, received or stored in a computer, electronic mail, telegram, telex or telecopy. Article 5 of the Model Law provides that information shall not be denied legal effect, validity or enforcement solely on the grounds that it is in the form of a data message. The criteria for assessing integrity shall be whether the information has remained complete and unaltered.

In assessing the evidential weight of data message, regard shall be had to the reliability of the manner in which the data message was generated, stored and communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified.[206]

[206] Article 9(2) of the Model Law.

Article 8 provides that where the law requires that information be presented or retained in its original form, that requirement shall be met by a data message if there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form.

3.7.3 General Appraisal

Regulating on the law relating to electronic commerce will play a greater role in addressing some aspects of electronic fraud and in particular electronic banking fraud. It is without a doubt that many banking transactions are now being transacted electronically and as such, both the banking institutions and the customers need to know that the law protects such transactions and is able to address any obstacle that may arise in the course of such transaction.

As a result of the increased use of technology, fraudsters too exploit the same to siphon money from banks and unsuspecting individuals. The UNICITRAL Model Law would to an extent assist in curbing of fraud since the law lays a lot of emphasis of recognition of electronic transactions and according them the same status as paper based transactions. Consequently, a person prove of electronic banking fraud by means of electronic data and evidence would assume the same relevance and weight just like any other kind of proof.

A person can for example, show that a fraudster used a certain electronic document or data such as use of emails to induce another to reveal pertinent information necessary in the commission of fraud. Section 106B of the Evidence Act[207] has however incorporated substantially all the aspects of admissibility of electronic records and data. Whereas this is commendable there is still need to legislate on a law that specifically deals with various aspects of electronic commerce with the sole aim of facilitating electronic communications.

[207] Chapter 80 of the Laws of Kenya.

3.8 THE BANKING FRAUD INSTITUTIONAL FRAMEWORK

There are a number of institutions in Kenya mandated with the responsibility of fighting electronic banking fraud. The police and the office of public prosecution play a major role in apprehension, investigation and prosecution of suspects. However, there are specialized agencies that specially address concerns on banking fraud. The Central Bank of Kenya has the Anti-Banking Fraud Unit which is a department in the Criminal Investigation Department (CID) whose core mandate is to investigate banking fraud in the country.

The investigation commences when the banks refer the cases to the Anti-Banking Fraud Unit. Before such referrals, the banks undertake their own investigations and assess whether it's worthwhile to refer those cases for further investigation. The end result is that, not all cases are taken up by the Anti-Banking Fraud Unit since banks are hesitant to refer all cases of suspected fraud especially on internal fraud in order to avoid the reputation risks involved.

The CID also has Cyber Crime Unit that specifically investigates any fraud allegedly committed through use of electronic gadgets. In such a case the first step is normally to inform the Anti-Banking Fraud Unit of the CID who first establishes that a crime has been committed. Once the crime scene is identified for example if it is a computer within the banking hall, the investigators from the Cyber Crime Unit will then be called upon to collect any material (software etc) necessary to unearth the fraud committed.

The Cyber Crime Unit has sufficient machinery necessary to investigate and apprehend the perpetrators of electronic banking fraud.[208] However, the Unit lacks the necessary human resource capital being people specially trained to investigate high level fraud cases especially those committed by use of technology. Generally investigators employed

[208] This was the view of one of the officer in the Cyber Crime Unit with the rank of an Inspector General interviewed on 13th September, 2013.

therein are normally police officers who in most cases lack requisite knowledge necessary to tackle the crime of fraud. Consequently, there is need to employ more specialist in order to ensure proper and thorough investigations. Additionally, there is need to offer relevant training to the existing investigators to keep them abreast with the everyday mutations of the crime of fraud.

3.9 CONCLUSION

Electronic banking fraud in Kenya has mainly being dealt with as a crime. Indeed, the predominant legislation discussed herein such as the Penal Code and the Kenya Information and Communications Act only provide for criminal sanctions. The Banking Act has however provided for other remedies such as removal from office in case of an officer who is found guilty of fraud and disqualification from holding office in any financial institution. This study has acknowledged that such additional remedies provided in the Banking Act are likely to have a more deterrence effect unlike the mere imposition of minimal fine or imprisonment. In any case, the penalties provided in most of the legislation are insufficient to deter offenders due to their high level of leniency.

Whereas the Penal Code predominantly deals with the traditional offences, the Code may still accommodate electronic banking fraud which is modern. The study highlights the offence of theft, obtaining by false pretenses and forgery as the main offences under which a fraudster may be charged with. This shows that, to this extent the law is flexible enough to be applied to new situations especially brought about by technology. There is however, still, the need to have specific laws specifically tailored to address the unique and dynamic characterization of the offence of electronic banking fraud brought about by use of technology.

The relevant legislations do not sufficiently address the electronic banking fraud. Irrespective of the 2009 amendments to the Penal Code and the Kenya Information and Communications Act, which amendments were specifically geared towards addressing crimes perpetrated through use of technology there is still a need to relook at some of the

provisions therein with an aim of expanding the scope of the regulated offences. For example, there is need to craft a well detailed definition of the term 'property' which incorporates both intangible and tangible property.

The Kenya Information and Communications Act (KIC) on the other hand has embraced the manifestation and nature of electronic banking fraud by specifically legislating against computer related crimes. The KIC Act serves as a supplement to the Penal Code in terms of addressing various forms and nature of electronic banking fraud that goes way beyond the characterization of related offences as provided for in the Penal Code.

The chapter has also highlighted the place of the law of tort in combating electronic banking fraud. The study proposes that there is need to pay more attention to the potential of civil remedies in fighting electronic banking fraud. Civil remedies are likely to be more effective due to their compensatory nature and the fact that the aggrieved person is wholly in charge of prosecuting the offender. However, banks are hesitant to result to civil law especially where the loss suffered can be compensated by the insurance.

Additionally, technology induced crimes are unique in the sense that the method of achieving a certain end result differs from the traditionally accepted modes of commission of offences. This therefore calls for unique laws tailored to specifically address such unique and dynamic ways of committing fraud. With such uniqueness therefore, there is need to clarify certain provisions of the current law so that all ways and manner of committing fraud are foreseeable and flexible enough to cover up even new and emerging tactics.

The banking institutions also have a larger responsibility of adhering to the CBK guidelines occasionally issued to them. They also need to keep abreast with the best practices originating from other jurisdictions in order to shield themselves from the occurrence of electronic banking fraud. In doing so, the UNICITRAL Model Law would play a very vital role by stipulating guiding principles that incorporates internationally accepted best practices.

CHAPTER FOUR

LEGAL REGIME IN OTHER JURISDICTIONS

4.1 INTRODUCTION

This chapter looks at how other jurisdictions address electronic banking fraud. It is an examination of how the following jurisdictions namely; the United Kingdom, Australia, South Africa and the United States have dealt with certain offences related to electronic banking fraud. The purpose is to find out their effectiveness in combating electronic banking fraud and finding out whether there are any relevant lessons Kenya can learn therein. The chapter thematically analyses certain offences from the named jurisdictions with an aim of finding out the effectiveness and sufficiency of the applicable laws.

The legal regime of the UK, South Africa and Australia is quite similar with Kenya since they all belong to the commonwealth. This chapter examines whether these jurisdiction have made any notable steps in enacting laws aimed at addressing electronic banking fraud. The US too provides an insight as to the applicable laws in addressing banking fraud. The chapter examines whether the US laws are comprehensive and robust enough in their attempt to fight electronic banking fraud.

4.2 Theft

Section 1 of the Theft Act (1968), United Kingdom defines the general offence of theft in the following words:

> "A person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it; and 'thief' and 'steal' shall be construed accordingly."

Section 4(1) the Theft Act defines property as money and all other property, real or personal, including things in action and other intangible property. This is an all inclusive

definition in that it defines property to encompass all other property, real or personal meaning that the scope of interpretation is widened.

The definition of the term property in the Penal Code is however restrictive in that it lists the kind of property contemplated therein consequently excluding all other forms of property not included therein.[209] Particularly, the Code does not include intangible property in the definition of the term property. Kenya can therefore adopt the definition of the UK in defining 'property' so as to include intangible property and choses in action but at the same time leave the scope wide enough for other form of property not specifically mentioned. For instance, by defining property to include all forms of intangible property and things in action.

4.3 Obtaining Property by Deception

Section 15(1) of the UK Theft Act, provides for the offence of obtaining property by deception whereby a person by deception dishonestly obtains property of another with the intention of permanently depriving the owner of it. This section is relevant in the offence of fraud because the act of fraud consists of dishonest conduct or false misrepresentation which induces another to act in a way that they would not have ordinarily acted.

In the case of *R v Preddy*[210] the appellants were charged under section 15 of the Theft Act, for obtaining property by deception. The appellants, in order to obtain mortgage advances, submitted applications containing false statements to building societies and lending institutions. On the strength of the false applications, sums were advanced to the appellants in the form of telegraphic or electronic transfer or by cheque. The appellants were convicted of obtaining "property belonging to another" by deception, contrary to section 15 Theft Act 1968 (UK). The House of Lords was asked to decide whether the debiting of a bank account and the corresponding crediting of another's bank account brought about by dishonest misrepresentation amounted to the obtaining of property within section 15.

---

[209] Section 2 of the Penal Code.
[210] (1996) AC 815.

The House of Lords held that, that does not amount to obtaining property belonging to someone else. Lord Goff in furtherance to this stated that:

> "When the bank account of the defendant is credited, he does not obtain the lending institution's chose in action. On the contrary that chose in action is extinguished or reduced pro tanto, and a chose in action is brought into existence representing a debt in an equivalent sum owned by a different bank to the defendant or his solicitor."[211]

In other words, the 'property' which the defendant acquired cannot be identified with the property which the lending institution lost when its account was debited. Consequently, the electronic funds transfer did not meet the threshold of 'property belonging to another' requirement in section 15(1).

This is because in any such transfer of intangible property from one person to another, the chose in action held by the transferor is destroyed, and an identical but separate and new chose in action is created in favour of the transferee.[212] This means that it may not be possible to obtain a chose in action that belongs to another.[213] The crux of this decision was that when money is transferred between accounts there is no identifiable property belonging to another that exists.

4.4 Fraud Act, 2006

The above case of *R v Preddy* exposed the lacuna that existed in the law namely that as much as money held in an account is an intangible property in the form of a chose in action, it may not be possible to have a chose in action belonging to someone else since after every transaction the old chose in action is destroyed and a new one created.

Consequently, the Law Commission of England and Wales recommended an amendment to section 15 of the Theft Act, 1968. The initial proposal was to provide for a new

---

[211] Ibid at 834.
[212] Ibid at 834, 835–7.
[213] Steel Alex, "Problematic and Unnecessary? Issues with the Use of the Theft Offence to Protect Intangible Property" *Sydney Law Review* 30 (2008): 575,590.

offence of obtaining a money transfer by deception.[214] However, the Law Commission settled on repealing some of the offences in the Theft Act and enacted the Fraud Act, 2006 which provided for general fraud offences. [215] The Act created an offence of fraud which can be committed in three ways namely, fraud by false representation, fraud by failing to disclose information and fraud by abuse of position.

Section 2 of this Act provides for fraud by false representation. A person is liable if he dishonestly makes a false representation with intention of making gain either for himself or another or to cause loss to another or to expose another to a risk of loss. A representation is false if it is untrue or misleading and the person making it knows it to be untrue or might be untrue or misleading. Section 5 defines gains or loss to include gain or loss of money or other property whether real or person including things in action and other intangible property.

This section ensures that the intangible property in question need not be property belonging to another. All that a person needs to prove is that there was a false representation and consequently a gain to the maker of the representation or loss to someone else. This could be loss of money, property etc. The phrase "obtaining property belonging to someone else" was deleted.

In addition, section 2 makes it an offence to commit fraud by false representation in any form. This section is applicable against a person who sends emails to large groups of people falsely representing that the email has been sent by a legitimate financial institution.[216] This is commonly referred to as phishing. Such emails prompt the reader to provide information such as credit card and bank account numbers so that the "phisher" can gain access to their assets, for example money held in the customer's account or confidential information.

---

[214] The Law Commission of England and Wales, "Offences of Dishonesty: Money Transfers" Law Commission (1996) 243 at [3.14].

[215] UK, Home Office circular 042 / 2006,*The Fraud Act 2006: repeal of the deception offences in the Theft Acts 1968 – 1996 (*2006) https://www.gov.uk/government/publications/the-fraud-act-2006-repeal-of-the-deception-offences-in-the-theft-acts-1968-1996 (visited 9th October 2013).

[216] *Ibid.*

Section 6 makes it an offence to possess articles for use in the course of any fraud or in connection with any fraud. A person would therefore be held liable under this section if they are found in possession of devices commonly used to copy credit card and debit cards details or software commonly used to copy passwords and PIN numbers among other likely articles.

4.5 Other Money Transfer Offences

The impact of *R v Preddy*[217] prompted several other jurisdictions to enact specific legislations in order to address the offence of electronic funds transfer.[218] For example, the federal State of Australian Capital Territory in Australia[219] enacted the Criminal Code 2002 which provided under section 330 the offence of obtaining property belonging to another where a person transfers money from one account to another.[220]

New South Wales, a federal state of Australia has on the other hand enacted specific money transfer offences. In 1979 offences of obtaining money or financial advantage by deception were created under section 178BA and 178 BB of the New South Wales Crimes Act, 1900. These were meant to fill gaps in law brought about by the original offence of obtaining by false pretense which had similar weaknesses like the offence of obtaining by deception in the UK.[221]

Section 178BA penalizes the obtaining by deception of any money, valuable thing or "any financial advantage of any kind whatsoever". The section defines "deception" to include both deliberate or reckless words or conduct and if by words includes representations of law as well as fact.

---

[217] (1996) AC 815.

[218] Alex Steel, "Problematic and Unnecessary? Issues with the Use of the Theft Offence to Protect Intangible Property." *Sydney Law Review* 30 , (2008): 575,592.

[219] Australian Capital Territory is a federal territory on the continent of Australia in the South East part within New South Wales. Online at http://www.thefreedictionary.com/Australian+Capital+Territory (Visited 9th October 2013)

[220] Previously in the Australian Capital territory, the offence against property was based on the common law offence of Larceny. Alex Steel, "Problematic and Unnecessary? Issues with the Use of the Theft Offence to Protect Intangible Property." *Sydney Law Review* 30 , (2008): 575,576.

[221] Judicial Commission of New South Wales, *False or Misleading Statements* (2002) online at http://www.judcom.nsw.gov.au/publications/benchbks/criminal/false_or_misleading_statements.html (visited 3rd Oct 2013).

The definition is also extended to include causing a computer system to make a response and an act or omission with the intention of causing a machine "designed to operate by means of payment or identification" to make an unauthorized response, thereby creating an offence of "deceiving" a machine, such as putting foreign coins into a slot machine or obtaining money through an automatic teller machine (ATM). There is, however no definition of financial advantage.

The elements of the offence of obtaining by deception under Section 178BA as discussed in the case of *R v Licardy*[222] includes obtaining by deception or dishonestly a financial advantage or money whether for one's benefit or for the benefit of another. The deception must have induced in the owner of the money an intention to part with his or her property rather than merely the custody or control of the money or financial advantage in question. This means that a person can be held liable under this section for dishonestly transferring money from the victims account to an account over which he has control.

Section 178BB on the other hand deals with recklessly obtaining money or financial advantage of any kind whatsoever. This can be contrasted with the definition of deception under section 178BA which includes the words "deliberate" or "reckless." The case of *Pollard v Commonwealth DPP*[223] held that, the prosecutor must prove beyond reasonable doubt that the accused made the statement not caring whether it was true or false and without any honest belief in its truth.

In the United States, the Computer Fraud and Abuse Act,1986 (CFA) prohibits any person from intentionally accessing a computer or electronic communication without authorization and obtaining financial, medical, or other proprietary information.[224] The CFA also prohibits any person from using a computer or electronic communication to:

i. Commit fraud;
ii. "trespass" on a protected computer;

---

[222] unrep, 28/09/94, NSWCCA.
[223] (1992)28 NSWLR 659.
[224] Computer Fraud and Abuse Act, 18 U.S.C.A. Section 1030(a)(2)(C).

iii. transmit programs, information, calls, or commands that intentionally cause damage to a protected computer; and
iv. to traffic in unauthorized passwords.[225]

"Protected computers" are computers used for private or commercial business purposes which transverse interstate lines for communication or commerce. In *America Online, Inc. v. LCGM, Inc.,* a Virginia federal district court held that, the use of the internet to send unauthorized and unsolicited bulk e-mail advertisements (i.e. "spamming") to customers in numerous states violated the CFA.[226] The court reasoned that the practice of spamming was considered an interstate communication and thus fell within the scope of the CFA. Moreover, the CFA provides civil claims for compensatory economic damages and injunctive or other equitable relief.

4.6 Computer Misuse Act, 1990

This Act was amended in 2006 by the provisions in the Police and Justice Act and further amendments introduced in 2007 by the Serious Crime Act. The relevant provisions of this Act as amended include;

a. Unauthorized access to computer material. Section 1 of the Act provides that a person is guilty of an offence if he causes a computer to perform any function with intent to secure access to any program or data held in any computer; the access he intends to secure is unauthorized and he knows at the time when he causes the computer to perform the function that is the case.
b. Unauthorized access with intent to commit or facilitate further offences. By section 2(3) it is immaterial whether the further offence is to be committed at the time of access or on some future occasion. This offence captures a scenario where a person may gain access into a computer in order to copy someone else bank details for purposes of committing fraud when an opportunity arises.

---

[225] *Ibid.*
[226] See American Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 449-52 (1998).

These offences are similar to the ones contained in the Kenya Information and Communications Act. However the offence of unauthorized access with the intention of committing a crime in the Kenyan context does not include access with intention of committing or facilitating further offences. However, I think that that offence can still be interpreted to include a scenario where one gains access to some confidential information and uses that knowledge to perpetrate electronic banking fraud at some future time.

4.7 Data Protection Act, 1998

This Act replaced the Data Protection Act, 1984. The objective of the Act is to regulate the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. It defines data to include *inter alia* information which is being processed by means of equipment operating automatically in response to instructions given for that purpose or which is recorded with the intention that it should be processed by means of such equipment.

Personal data includes information which relates to a living individual who can be identified from those data, or any other information which is in the possession of, or is likely to come into the possession of, the data controller. Personal data may be identified to one or more individual. The data subject is entitled to certain rights with regard to their data. The main purpose of the Act is to protect the privacy of the individual information either held by him or someone else. The question then is whether this law can be applied in electronic banking fraud as a result of breach of privacy which results in access to confidential information which information may then be used to commit electronic banking fraud. From my reading of the Act and the assessment of the various materials on the Data Protection Act, it seems that the issue as to whether the Act may be useful in combating electronic banking fraud or fraud generally had not been explored.

Many commentaries of the Act are on the extent of the Act to protect the right of privacy especially individual privacy which borders on the line of defamation as opposed any likely commission of fraud. This may be attributed to the fact the UK has various other

statutes that deals with fraud generally or electronic banking fraud particularly as already discussed above. However the fact that individual data is protected by the Act whether in possession of that individual or someone else it equally means that a fraudsters may be prosecuted under the Act where he accesses an account's holder information whether or not he subsequently that information to commit fraud.

4.8 Regulation against Spam messages and computer related offences

The Australian Spam Act, 2003[227] prohibits the sending of unsolicited commercial electronic messages.[228] A commercial electronic message is an electronic message the purpose of which is to advertise, promote or offer to supply goods or services; to advertise or promote a supplier of goods or services; to advertise, promote or offer to supply land or an interest in land; to advertise or promote a supplier of land or an interest in land; to advertise, promote or offer to provide a business opportunity or investment opportunity; or to advertise or promote a provider of a business opportunity or investment opportunity. The main remedies provided herein are civil remedies in the form of compensation for damages suffered and injunctions.[229]

Electronic banking fraud may occur when fraudsters send unsolicited commercial messages which purports to originate from a genuine financial institution. For example, information advertising banks products or other opportunities. This could be in the form of email messages which have links to fraudulent websites. Once the customer click on the links provided they are induced into revealing confidential information which they do on the belief that they are dealing with the genuine institution. The fraudster is then able to access the customer's account using the information obtained.

Similarly, Section 45 of the South African Electronic Communications and Transactions Act, 2002, legislates against sending of unsolicited commercial communications to consumers. The Act protects against the unlawful collection of customer information. For

[227] This is a federal government statute.
[228] Section 6 of the Spam Act.
[229] See Part 4 of the Act.

instance, it is an offence to electronically request, collect or store personal information that is not necessary for the lawful purpose for which the personal information is required. Fraudsters mainly send spam messages with the motive of gaining unauthorized personal information. This Act therefore regulates against such activities and persons found liable risks being fined or imprisoned for a period not exceeding 12 months.

Common law is also applicable in South Africa in resolving some of the technology related frauds in the criminal regime. For instance, courts, through case law, have been able to find that misrepresentation, which is a crucial element of fraud, can be made to a computer or other electronic gadgets[230].In *S v Myeza 1985 (4) SA 30 (T),* the accused was found guilty after he had placed a counterfeit coin or object into a parking meter. The misrepresentation in this case is made to the parking meter, and not a person. However, it can be said that the representation was to the persons in charge of parking. By the same reasoning, it would be in order to deduce that a misrepresentation to a computer or another electronic gadget can be said to be a misrepresentation to the bank or owners of the machine.

Similarly in the case of *S v Van den Berg 1991 (1) SACR 104 (T)* the accused unlawfully credited R800 to his account through a computer terminal. This was held to be a misrepresentation to the bank. In addition, the court stated that, a misrepresentation done electronically into the computer system was the same as where a bank clerk makes a written false entry into the accounting records.

In the United States, there are a number of information security laws that are designed to protect personally identifiable information or sensitive personal information from compromise, unauthorized disclosure, acquisition, access, or other situations where unauthorized persons have access or potential access to personally identifiable

[230]P Carstens & A Trichardt, " Computer Crime by Means of the Automated Teller Machine – Just Another Face of Fraud?" *SACC* (1987),131.

information for unauthorized purposes[231]. In seeking to protect information, US information security laws have put in place state monitoring mechanisms of institutions that hold information such as banks.

For instance, the Privacy Act, 1974 requires that when agencies establish or modify a system of records, they should publish a "system-of-records notice" in the Federal Register[232]. The notice to the Federal Register must have information on the type of data collected, the types of individuals from whom data has been collected, the intended uses of data and procedures that individuals can use to review and correct personal information[233].

The Gramm-Leach-Bliley Act of 1999 is the statute that specifically addresses information security for financial institutions. It requires financial institutions to provide their customers with notice of their privacy policies. It also requires financial institutions to safeguard the security and confidentiality of customer information in order to protect against any anticipated threats including fraud[234]. The information protected under this Act is all inclusive. Customer information is defined as:

> *"Information about a customer, whether in paper, electronic, or other form, that is maintained by or on behalf of a financial institution."*

There is also an aspect of industry self-regulation in information security in the U.S. The Payment Card Industry Data Security Standard, for instance, has been set by the payment card industry[235]. It has set security standards for all players in that industry[236]. It requires organizations that handle bank cards to conform to security standards and follow certain

---

[231] Gina Stevens, Federal Information Security and Data Breach Notification Laws, Congressional Research Service 7-5700 www.crs.gov RL34120, p 1.

[232] 5 U.S.C. § 552e(4).

[233] the type of data collected, the types of individuals about whom information is collected, the intended "routine" uses of data, and procedures that individuals can use to review and correct personal information. 5 U.S.C. § 552e(4).

[234] 15 U.S.C. § 6801 - 6809. See CRS Report RS20185, Privacy Protection for Customer Financial Information, by M. Maureen Murphy.

[235] https://www.pcisecuritystandards.org/security_standards/role_of_pci_council.php (Accessed on 8th October 2013).

[236] The standard was developed by VISA, MasterCard, and other bank card distributors in the United States of America.

leveled requirements for testing and reporting. The principal objective is to establish and sustain a secure network, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, monitor and test networks, and maintain an information security policy[237].

Organizations do not comply by the industry regulation face punishments such as fines and increases in the rates that the credit card companies charge for transactions, and potentially can have their authorization to process payment cards revoked[238].

4.9 Liability in fraud

In South Africa, the credit card relationship is governed by the contract between the customer and the issuer as provided in the National Credit Act 34 of 2005[239]. The general rule under the Act is that the cardholder bears all the risks for unauthorised transactions until the issuer is informed, where after the issuer will bear the loss[240].

In *Diners Club SA (Pty) Ltd v Singh and another 2004 (3) SA 630*, an account holder was found guilty for authorizing certain transactions that occurred with his card in London. The court held that an original card and pin were used to perpetrate the fraud and not a duplicate card. The court however pointed out that the contract was one-sided and favoured the card issuer, so that the risk of wrongful use is placed on the customer[241].

4.10 Conclusion

It is evident that the stated jurisdictions have enacted specific laws with an aim of curbing electronic banking fraud. Some of the federal states of Australia like the New South Wales and the Australian Capital Territory have amended their general criminal laws to broaden their scope in order to accommodate the offence of electronic banking fraud. The

---

[237] https://www.pcisecuritystandards.org/security_standards/role_of_pci_council.php (Accessed on 8th October 2013).

[238] *Ibid.*

[239] Charnelle van der Bijl, "The cloning of credit cards: The dolly of the electronic era," Stellenbosch Law Review, 18 no. 2 (2007), 338.

[240] *Ibid.*

[241] In *S v Salcedo 2003 (1) SACR 324 (SCA)*, the accused committed credit card fraud by picking up a credit card that had fallen out of the account holder's pocket in a mall and going on a spending spree the same day. The accused was convicted on nine counts of fraud and sentenced to six months imprisonment on each count.

UK on the other hand has enacted a general fraud legislation that encapsulates the offence of electronic banking fraud as well as the Computer Misuse Act and the Data Protection Act. Similarly, the US and SA have enacted specific laws aimed at curbing computer related offences.

The chapter contains relevant lessons that Kenya can learn in its fight against electronic banking fraud. Just like the UK and Australia, there is need to expound on the definition of the term 'property' so as to provide for intangible property. Kenya can also enact specific laws on fraud without necessarily amending its Penal Code. This could be a general fraud legislation or different legislations that regulates against specific ways of commission of electronic banking fraud. For example a Spam Act that regulates against sending of unsolicited messages whether commercial or non-commercial and a Computer Abuse legislation that regulates against all form of computer abuse including hacking or any form of misrepresentation that involves use of computers would be necessary.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.1 CONCLUSION

Chapter 2 of this study has revealed the nature of electronic banking fraud both as a crime and a civil wrong. This means that remedies lie both in the criminal law and in civil law. Electronic banking fraud is fraud that is perpetrated through use of various banking technologies. This fraud manifests itself in various forms including *inter alia*: identity fraud, payment card fraud and hacking.

Electronic banking fraud in Kenya is mainly being dealt with as a crime. The Penal Code and the Kenya Information and Communications Act, are the predominant legislation that seek to address electronic banking fraud. The only remedies provided therein are criminal sanctions.

This study has established that the Penal Code, though dealing predominantly with traditional offences still accommodates some aspects of electronic banking fraud which have similar characteristics with the other offences. Some of these offences includes: the offence of theft, obtaining by false pretenses, conspiracy to defraud and forgery.

Though the Penal Code accommodates to some extent the prosecution of electronic banking fraud, new forms of technology driven offences will always emerge due to changes in technology. Consequently it is important to expound the definition of some of the crimes to make them flexible enough to accommodate these ever emerging crimes.

The Kenya Information and Communications (Amendment) Act of 2009, on the other hand, regulates against various computer induced crimes. While this is major progress made in the fight against electronic banking fraud, there is still room for further development of the law. It is worth noting that this Act was enacted to facilitate development of electronic commerce by specifically establishing the institution of

Communications Commission of Kenya now Communications Authority of Kenya. The provisions on misuse of computers discussed under Chapter 3 were only introduced through the 2009 amendments and as discussed therein are insufficient. Indeed, this study has revealed that Kenya lacks adequate national laws necessary to curb electronic banking fraud. The UNCITRAL Model Law on electronic commerce may provide some guidance towards legislating on the relevant legislation. It provides for the internationally agreed standards and principles to be taken into consideration when legislating.

5.2 RECOMMENDATIONS

5.2.1 Amendments

I recommend the following amendments:

5.2.1.1 Definition

a. Penal Code

The definition of the term 'property' as provided for under section 2 of the Penal Code should be amended to include intangible property. This is because electronic banking fraud mostly manifests itself in terms of loss of a chose in action namely money held in an account which is intangible property. Currently, it is not possible to charge a person for theft of money held in an account for instance after an electronic fund transfer, since such money is not considered as property belonging to another and neither is it a thing capable of being stolen.

Additionally, money held in a bank account should be included under Section 267 of the Penal Code as a thing capable of being stolen. This is because the offence of theft requires that one takes something which is capable of being stolen. Consequently, if a fraudster transfers money from one account to another, he cannot be said to have stolen that money since money held in an account is not capable of being stolen.

The offence of theft should not be tied to the aspect of intentionally depriving the owner permanently of the thing stolen. In this regard, Kenya can adopt the UK elements of

fraud, being, an act that results in a gain for the fraudster and a loss to the victim. This is because in some cases especially with regard to electronic banking fraud there may not be actual deprivation on the owner of the thing stolen. Of relevance here is if a person hacks into a computer and copies data stored in it without necessarily deleting it. That kind of theft would not qualify as 'theft' under this provision since the owner is not in any way deprived of the confidential information.

b. Kenya Information and Communications Act

There is need to define the term 'property' in the KIC Act. Various provisions in the Act refer to the term 'property' with no actual definition in the Act. For example, Section 84B regulates against fraudulently causing loss of property of another by input, alteration, deletion or suppression of any data or any interference with a computer system. The key word here is 'loss of property' notwithstanding the fact that the term 'property' has not been defined. This study proposes a definition of the term 'property' which is comprehensive enough to include every form of physical and intangible property, anything which a person can place a money value on it. This would ordinarily include information both stored in the computer and the programming instructions that allow a computer to function. There is even a greater need to define the term 'fraudulent'. The Act has so many provisions on fraudulently causing loss of property without defining the meaning of that term.

The Act should also be amended to include civil remedies for offences committed under the Act. Examples of these include injunction, damages for loss sustained and other relevant reliefs. These kinds of remedies would ensure that a fraudster pays up compensation for the loss caused. An aggrieved party would therefore be able to institute civil proceedings and claim compensatory damages under the Act. The advantage of such proceedings would be not only the ability to get actual compensation but the fact that the victim would be able to prosecute their case under civil law. This would ensure that the victims, whether a bank or individual are in control of the prosecution unlike in criminal

cases. Additionally, especially for the banks, they are likely to have better machinery in terms of money and access to legal advice necessary to advance their cause.

5.2.1.2 Enhancing of Criminal Sanctions

Most of the fraud related offences under the Penal Code and under the Kenya Information and Communications Act attracts a minimal penalty. For example, the offence of obtaining by false pretences and theft under the Penal Code attracts a penalty of three years imprisonment. On the other hand, a person who causes unauthorized modification of computer data under the KIC Act is liable to a fine not exceeding 50,000/-.

The penalties herein do not necessarily commensurate with the level of damage caused. This study recommends that a person should be fined an amount equivalent to the loss occasioned. For example, if someone defrauds a bank an amount equivalent to Kenya Shillings 300 million then such a person should in addition to imprisonment be fined an equivalent amount. That way a person will not live off through the proceeds of crime.

Further, the three (3) years imprisonment provided is insufficient as fraudsters are able to quickly serve their jail term and later gets to enjoy the money stolen. Whereas others argue that stiff penalties do not necessarily deter offenders and the case in mind is the imposition of death penalties to the capital offenders. My argument is that, to some extent people will ordinarily fear committing a particular offence when they know the penalties are harsher. People are normally rational individuals who weigh the options available before committing an offence.

5.2.1.3 Alternative Sanctions

In addition to the criminal sanctions provided in the Penal Code and the KIC Act, there should be other sanctions in the form of public condemnation in terms of media advertisement setting out details of the corporation's or individual's criminal conduct. These kinds of sanctions would be more appropriate in deterring corporations and high level individuals whose image is likely to be damaged by any public condemnation. For

example, if a corporation through its management aid in commission of fraud, then if found liable it should be legally compelled to report to the shareholders through annual report the rate of the occurrence of fraud in its institution.

This kind of sanction is likely to have a higher deterrent level since corporations are very keen on maintaining a good public image. Consequently, in order to avoid acts of public outcry which can even lead to public boycott on their products, corporations are likely to ensure that their institutions are not used as avenues for commission of fraud. They are therefore likely to put up relevant measures which are strictly adhered to in curbing of electronic banking fraud. This is likely to curb instances of internal fraud.

5.2.2 Enacting a General Fraud law

My study recommends that just like the UK, Kenya should enact a specific legislation against fraud. The starting point would be to firstly define various elements which would be said to constitute fraud. Further the Act should elaborate that the fraud may be committed either by omission or commission. The advantage of enacting such a law would be to capture all aspects of fraud whether done through the use of technology or otherwise. This would also prevent a scenario where there is legislation in all contemplated means of committing electronic banking fraud such as legislating against sending of spam messages, hacking among others.

5.2.3 Enhancing Capacity to the Banking Fraud Institution

There is need to empower relevant institutions tasked with the responsibilities of investigating and prosecuting electronic banking fraud. For example the Central Bank Anti-Banking Fraud Unit of the Criminal Investigation Department needs human resource capacity in terms of trained personnel necessary to undertake sophisticated investigation of electronic banking fraud. Majority of the investigators are police who lack sufficient skill and knowledge necessary to address the emerging complexities of the crime of electronic banking fraud.

5.2.4 Public sensitization

The public needs to be educated on its role in combating electronic banking fraud. To begin with, not all fraud cases are reported. The usual practice is that once a person realizes that they have been defrauded, they report to their bank. The bank will then conduct its own investigation and determine whether such a case warrants being referred to the Anti- Banking Fraud Unit. Consequently, not all cases are reported especially with regard to internal fraud cases since the banks fear having a reputational back lash. The public needs to be vigilant and report to the Anti-Banking fraud Unit any occurrence of a banking fraud so that each and every case is investigated and if need be prosecuted. This will send a strong message to the fraudsters and potential offenders that that the justice system is working.

5.3 CONCLUSION

This study has highlighted some of the proposed recommendations in the fight against electronic banking fraud. There are loopholes in the laws against electronic banking fraud. This study has highlighted areas of law of relevance to the policy makers that need to be reexamined.

BIBLIOGRAPHY

Books

Alridge Anthony & Milne Alexander, *Alridge & Parry on Fraud*, 3rd ed. (London: Sweet & Maxwell 2011)

Buys Reinhardt & Buys Francis, *Cyberlaw,The Law of Internet in South Africa*, (Pretoria: Van Schaik Publishers, 2004)

Chorafas N Dimitris, *Electronic Funds Transfer* (London: Butterworths, 1988)

Chitty Joseph, *Chitty on Contracts* 22nd ed Vol 1.(London: Sweet & Maxwell, 1961)

David Ormerod, *Smith and Hogans's Criminal Law* 13th ed. (New York: Oxford University press, 2011)

Jones A.M, Dugdale M.A., *Clerk & Lindsell on Torts* 19th ed.(London: Sweet & Maxwell, 2005)

John G Fleming, *The Law of Torts* 9th ed. (North Ride: Information Services, 1998)

Michael Brindle & Raymond Cox, *Law of Bank Payments*, 4th ed. (London: Sweet & Maxwell, 2010)

Njaramba Gichuki, *Law of Financial Institutions in Kenya*, 2nd ed. (Nairobi: Law Africa, 2013)

Stephen, *A History of the Criminal Law of England*, vol. II (London Macmillan, 1883)

Journals

Akindemowo, Olujoke E "The Fading Rustle, Chink and Jingle: Electronic Value and the Concept of Money" *University of New South Wales Law Journal* 21, (1998):466

Basel Committee on Baking Supervision, "Management and Supervision of Cross-Border Electronic Banking Activities," *Bank for International Settlement* (July 2003)

Bohm Nicholus , Brown Ian & Gladman Brian, "Electronic Commerce: Who Carries the Risk of Fraud?" *Journal of Information, Law and Technology* 3, (2000)

Bollen Rhys, "The Development and Legal Nature of Payment Facilities." *Murdoch University Electronic Journal of Law* 11, no. 2 (2004)

Bonner et. al Sarah E. " Fraud Type and Auditor Litigation: An Analysis of SEC Accounting and Auditing Enforcement Releases." *The Accounting Review* 73, no. 4 (1998)

Biskupic Steven M., "Fine Tuning the Bank Fraud Statute: A Prosecutor's Perspective." *Marq. L. Rev.* 82 (1999)

Brenner Susan W, "Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law.") *Murdoch University Electronic Journal of Law*, 8, no. 2 (2001)

Bhatla Tej Paul, Prabhu Vikram & Dua Amita, "Understanding Credit Card Fraud." *Card Business Review*, (2003)

Beatty, Andrea; Aubrey, Mark; Bollen, Rhys "E-Payments and Australian Regulation" *University of New South Wales Law Journal* 21 no.2 (1998):489

Caminer F Brian, "Credit Card Fraud, the Neglected Crime." *Journal of Criminal Law and Criminology*76 no.3 (1985)

Chaikin, David, "A Critical Examination of How Contract Law Is Used by Financial Institutions Operating in Multiple Jurisdictions." *Melbourne University Law Review* 34 no.1 (2010)

Charnelle van der Bijl, "The cloning of credit cards: The dolly of the electronic era," *Stellenbosch Law Review*, 18 no. 2 (2007)

Carstens P & Trichardt A, "Computer Crime by Means of the Automated Teller Machine – Just Another Face of Fraud?" *SACC,* (1987)

D Kebbell, "Criminal Law: Theft and Fraud." 10 *Otago Law Review* (2001)

Douglas-Stewart Jeremy, "South Australian Laws target Identity Theft." *Privacy Law and Policy Reporter*, 8, (2004)

Dunning M., "Some Aspects of theft of Computer Software." *Aucklard University Law review*, (1978)

Farrar, H John. "Fighting Identity Crime." *Bond Law Review Article 23,* no.1 (2011)

Fisse Brent, "The use of publicity as a Criminal Sanction against Business Corporations." *Melbourne University Law review*, 8 (1971)

Gray Anthony, "Criminal Sanctions for Cartel Behaviour." *Queensland University of Technology Law and Justice Journal*,8 no.2 (2008)

Hemming Andrew, "A Tale of Abuse of Position and False Accounting." *UNDARL*, 11,(2009)

Ikechu Success Kanu & Okay Okorafor, "The Nature Extent and economic Impact of Fraud on Bank Deposit in Nigeria ." *Interdisciplinary Journal of Contemporary Research in Business* 4 no.10 (2013)

Jane Swanton, "*The Convergence of Tort and Contract.*" Sydney Law Review, 12, (1989)

Kassim Mohd and Bin Noor Mohamed, "Problems Faced by the Criminal Justice System in Addressing Fraud Commited by Multi national Corporations." *Internet Journal of Criminology* 26, (2006)

KD Kilonzo, "An analysis of the Legal Challenges posed by Electronic Banking." *Kenya Law Review* 1,(2007)

Loundy J David , "Computer Information Systems Law And System Operator Liability Revisited", *Murdoch University Electronic Journal of Law*, 3 no.1 (1994)

Mcleod Dane, "Regulating Damage on The Internet: A Tortious Approach?" 27 *Monash University Law Review*,346 (2001)

New Zealand Law Commission, "Review of the Privacy Act." *NZLC* (2010)

Owalabi SA,"Fraud and Fraudulent Practices in Nigeria Banking Industry." *African Research Review Journal,* 4. No. 3b (2001)

Peter Alces, "Toward a Jurisprudence of Bank-Customer Relations" *The Wayne Law Review* (1968)

Pontell Henry, "Identity Fraud, Cyber-Crime, and White- Collar Delinquency" *Adelaide Law Review* 23 (2002)

Ravi Vadlamani, "Introduction to Banking Technology and Management." Institute for Development and Research in Banking Technology, *IGI Global, India* (2008)

Steel Alex, "Problematic and Unnecessary? Issues with the Use of the Theft Offence to Protect Intangible Property."*Sydney Law Review* 30 (2008)

Savirimuthu Anne and Savirimuthu Joseph, "Identity Theft and System Theory: The Fraud Act 2006 in Perspective," *Scripted*,4 (2007)

Swanton Jane, "The Convergence of Tort and Contract." *Sydney Law Review*, 12, (1989)

Sullivan Richard, "The Changing Nature of U.S Card Payment Fraud: Industry and Public Policy Option.", *2nd Quarter Economic Review Federal Reserve Bank of Kansas City*, (2010)

Stewart Jeremy Douglas, "South Australian Laws target Identity Theft." *Privacy Law and Policy Reporter*, 8, (2004)

S.S.P, "Measure of Damages for Fraud and Deceit." *Virginia Law review* 47, (1961)

Tej Paul, Vikram Prabhu & Amita Dua, "Understanding Credit Card Fraud." *Card Business Review*, (2003)

Tucker Greg, "Electronic Payment System: Some Legal Issues." *Law Institute Journal* (1997)

The Law Commission of England and Wales, "Offences of Dishonesty: Money Transfers" *Law Commission* (1996)

Vries de Bald, Tigchelaar Jet & Tina van der Linden "Describing Identity Fraud: Towards a Common Definition." *Scripted* 5 (2008)

V Subha, "Retail Banking Fraud Management: Challenges and Emerging Alternatives." *TATA Consulty Services*, (2012).

Wilhelm Wesley K. & Fair I. Company, "The Fraud Management Lifecycle Theory: A Holistic Approach to Fraud Management." *Journal of Economic Crime Management Spring* 2, no.2 (2004)

Internet Sources

Ajayi M. A *Determinants of Fraud in Nigerian Banking Industry* Univerisity of Ilorin, Nigeria):101 online at http://www.unilorin.edu.ng/publications/ajayima/8.pdf

Leuchtner Tom,"4 Internal Fraud and how to Spot Them." http://www.ababj.com/briefing/4-internal-frauds-and-how-to-spot-them-1965.html

Moore Tyler and Clayton Richard, "Examining the Impact of Website Take-down on Phishing." p.2, http://lyle.smu.edu/~tylerm/ecrime07.pdf

Mugwe David , Kenyans Banks Biggest Victims Of Sh 4.1 bn Fraud, Business Daily, 31st July 2012 online at http://www.businessdailyafrica.com/Kenyan-banks-biggest-victims-of-Sh4bn-fraud-/-/539552/1467902/-/9kmes9z/-/index.html

Nyangosi Richard, Nyang'au Samuel and Magusa Hellen, "Managing Banks Amid Information and Computer Technology: Paradigms in Kenya." http://www.aibuma.org/archive/proceedings2011/aibuma2011_submission_43.pdf

"Pushing Banks from Old ATM Cards to High Security Chip and Pin Card Technology in Kenya, "CIO/East Africa Magazine, 6th November 2012 online at http://www.cio.co.ke/news/top-stories/pushing-banks-from-old-atm-cards-to-high-security-chip-and-pin-card-technology-in-kenya.

Rhoades and Sinon, "Electronic Banking Fraud." *www.rhoadssinon.com/media/site_files/35_PABanker%2001-02.pdf.*

Serianu Cyber Intelligence Team, *Kenya Cyber Security Report 2012, Getting Back to the Basics*, Ed 1, (2012) P 17, online at http://www.serianu.com/downloads/KenyaCyberSecurityReport2012.pdf

T. Tengku M, "Ethics of Information Communication Technology" A paper presented at the the Regional Meeting on Ethics of Science and Technology 5-7 November 2003, Bangkok. Online at http://www.unescobkk.org/elib/publications/ethic_in_asia_pacific/239_325ETHICS.PDF

Government Publications

Association of Certified Fraud Examiners, "The Fraud Trial: The Law Against Fraud" P. 6 available at http://www.acfe.com/uploadedFiles/Shared_Content/Products/Self-Study_CPE/Fraud-Trial-2011-Chapter-Excerpt.pdf

Central bank of Kenya, Kenya Electronic Payments and Settlement System, http://www.centralbank.go.ke/index.php/2012-09-21-11-44-41/kepss

Judicial Commission of New South Wales, False or Misleading Statements (2002) http://www.judcom.nsw.gov.au/publications/benchbks/criminal/false_or_misleading_statements.html

Kenya National Bureau of Statistics, *Economic Survey 2012 Highlights (*May 2012)

Milcah Kwambukha, Kenya Bankers Set Deadline for Chip and Pin Tech, Web Africa Published on 8th April 2013 online at http://www.itwebafrica.com/ict-and-governance/256-kenya/230841-kenya-bankers-set-deadline-for-chip-and-pin-tech

New Zealand Law Commission, "Are Changes to the Criminal Law needed?" http://www.commonlii.org/cgi-bin/disp.pl/nz/other/nzlc/report/R54/R543.html?stem=0&synonyms=0&query=%22altering%20a%20document%20%22

UK, Home Office circular 042 / 2006, "The Fraud Act 2006: repeal of the deception offences in the Theft Acts 1968-1996."(2006) https://www.gov.uk/government/publications/the-fraud-act-2006-repeal-of-the-deception-offences-in-the-theft-acts-1968-1996

US, PCI Security Standards Council, *What is the PCI Security Standards Council* https://www.pcisecuritystandards.org/security_standards/role_of_pci_council.php

Proceedings of Conference

O Kömmerling & M Kuhn, "Design Principles for Tamper Resistant Smartcard Processors', Proceedings of USENIX Workshop on Smartcard Technology, Chicago, USA, (May 1999)

United Nations Organization, United Nations Conference on Trade and Development (UNCTAD), *Transfer and Development of Technology in Developing Countries: A Compendium of Policy Issues*, (New York 1990)

Unpublished Sources

Egbune Okwute , "*Fraud and Forgery in the Nigerian Banking Industry: A Case Study of Staff Involvement*", (Ahmadu Bello Univeristy Zaria, Dept of Business Administration Sep, 1995)